Sistema de Vigilancia Tecnológica y Agentes Inteligentes

Carlos Rodríguez Fernández
<carlosrodriguez@computer.org>

Director:
Dr. Jorge Gómez Sanz
<jjgomez@sip.ucm.es>

Proyecto Fin de Master en Sistemas Inteligentes
Máster en Investigación en Informática, Facultad de Informática,
Universidad Complutense de Madrid
Curso 2008 - 2009

El/la abajo firmante, matriculado/a en el Máster en Investigación en Informática de la Facultad de Informática, autoriza a la Universidad Complutense de Madrid (UCM) a difundir y utilizar con fines académicos, no comerciales y mencionando expresamente a su autor el presente Trabajo Fin de Máster: "Sistema de Vigilancia Tecnológica y Agentes Inteligentes", realizado durante el curso académico 2008-2009 bajo la dirección de Dr. Jorge Gómez Sanz en el Departamento de Ingeniería del Software e Inteligencia Artificial (ISIA) , y a la Biblioteca de la UCM a depositarlo en el Archivo Institucional E-Prints Complutense con el objeto de incrementar la difusión, uso e impacto del trabajo en Internet y garantizar su preservación y acceso a largo plazo.

Carlos Rodríguez Fernández

Resumen

Los avances tecnológicos van incrementándose con el tiempo. El volumen de publicaciones científicas, patentes, proyectos de investigación, noticias de tecnología y normas internacionales relacionadas con las tecnologías va en incremento. Esto pone a disposición de investigadores, organizaciones de I+D+i, e industria en general, una enorme cantidad de información que analizar para sus proyectos y estrategias. Los Sistemas de Vigilancia Tecnológica son sistemas que se dedican a procesar la información tecnológica del entorno para extraer conocimiento, como es la identificación de tendencias y cambios. En este trabajo se estudia qué es un Sistema de Vigilancia Tecnológica haciendo incapié en el problema fundamental de evaluar y gestionar fuentes de información. Dada la naturaleza y objetivos de un sistema como este, se propone un diseño orientado a agentes para estudiar el impacto de una implementación concreta de modelos de confianza que ayude a gestionar fuentes de información.

Palabras claves. vigilancia tecnológica, sistemas autónomos, gestión de información, agentes inteligentes, confianza, reputación

Abstract

Technological advances are increasing with time. The volume of scientific publications patents, research projects, technology news and related international standards of technology is in continuous increase. This makes available to researchers, R+D organizations, and industry in general, a huge amount of information to analyze for their projects and strategies. Technology Watch Systems are involved in processing of all information technology environment to extract knowledge, such as identifying trends and changes. This paper studies the components of a Technology Watch System focusing on the information sources quality. It proposes an agent oriented design of a trust model for the management of information sources for its use within a Technology Watch System.

Keywords. technology watch, autonomous systems, information management, intelligent agents, trusting, reputation

Índice general

Índice de figuras

Índice de cuadros

Capítulo 1

Introducción

El ritmo de los avances científico-técnicos se incrementa con el paso del tiempo. Como consecuencia, ha aumentado considerablemente el ritmo de publicaciones científicas; proyectos de investigación, desarrollo e innovación; patentes; noticias de tecnología; y normas internacionales asociadas a tecnologías. A esto se une que los medios de comunicación actuales como Internet han permitido la rápida difusión de estos contenidos y por lo tanto, los investigadores, centros de I+D+i [1], y la industria en general, tienen a su alcance un enorme volumen de información que procesar y estudiar para marcar los rumbos de sus estrategias y proyectos.

Los Sistemas de Vigilancia Tecnológica se presentan como herramientas en los sistemas de gestión I+D+i [4]. Estos sistemas se encargan de detectar, analizar y explotar la información útil para una organización. Sobre todo, interesan avances e innovaciones científico-técnicas que puedan afectar a los proyectos y estrategias de la organización o puedan convertirse en oportunidades de negocios. Dichas informaciones se obtienen mediante la exploración semi-automáticas de fuentes de información dadas, y la colaboración de operadores humanos.

Los Sistemas de Vigilancia Tecnológica son sistemas que están continuamente vigilando y procesando contenido de fuentes de información. En el desempeño de sus labores, se espera de estos sistemas cierto grado de autonomía, ya que se quiere liberar a los operarios humanos de su carga de trabajo. Al mismo tiempo, se sabe que muchas de las tareas involucradas implican un uso intensivo de recursos. Por ello, al diseñar un sistema de vigilancia, es recomendable que partes de este se puedan ejecutar indistintamente en diversas máquinas. Estas dos características, la de autonomía y la de inherente distribución del trabajo, hacen pensar que la tecnología de agentes puede ser apropiada para diseñar este tipo de sistemas[21]. Los agentes software son programas diseñados para mostrar cierto grado de autonomía y para ejecutar sus labores en distintos entornos. Según sean las necesidades de computación y las disponibles en el entorno actual, un agente puede migrar a otro entorno más adecuado. Así pues, se parte de la hipótesis de que un diseño orientado a agentes puede facilitar reflejar requisitos de autonomía y computación distribuida de los Sistemas de Vigilancia Tecnológica.

Aparte de los anteriores, en el diseño de un Sistema de Vigilancia Tecnológica

[1] Investigación, Desarrollo e Innovación

aparecen diversos retos, entre los cuales se puede mencionar la obtención de la información desde fuentes heterogéneas; la valoración semiautomática de fuentes de información; el filtrado, la homogeneización, la clasificación y el priorizado de la información obtenida; la difusión de la información; y finalmente la preparación de informes de análisis de tendencias, identificación de cambios potenciales, recomendaciones, entre otros posibles informes que requiera la organización.

De los problemas antes mencionados, este trabajo se centra en gestión de fuentes de información y, concretamente, cómo se puede evaluar de forma automática su calidad sin coste computacional elevado. Es deseable que las fuentes a procesar por el sistema sean introducidas por los mismos investigadores de la organización. La calidad de una fuente propuesta al sistema depende de cuanto dedica un investigador a analizar dicha fuente y qué criterios aplica. El Sistema de Vigilancia Tecnológica debe ser capaz de realizar filtrados de las fuentes propuestas basados en valores de calidad calculados semi-automáticamente, y de optimizar el uso de filtrados que resultan muy costosos en tiempo y cómputo.

Siguiendo la hipótesis establecida anteriormente, este trabajo propone un diseño orientado a agentes de la parte de gestión de fuentes de información en un Sistema de Vigilancia Tecnológica usando como base un modelo de confianza adecuado.

1.1. Objetivos del Trabajo

Los objetivos de este trabajo son los siguientes:

- Estudiar qué es un Sistema de Vigilancia Tecnológica.
- Estudiar modelos de confianza para la evaluación de la calidad de fuentes de información.
- Proponer un diseño orientado a agentes de la gestión de propuestas de fuentes de información basado en un modelo de confianza en un Sistema de Vigilancia Tecnológica usando la Metodología INGENIAS [22] y el modelo de confianza REGRET.

1.2. Estructura del Trabajo

La estructura del trabajo es como sigue:

Capítulo 2. Se presenta formalmente lo que es un Sistema de Vigilancia Tecnológica introduciendo brevemente los problemas principales. Asimismo, se presentan varios modelos de confianza describiendo brevemente sus características.

Capítulo 3. Se propone un diseño orientado a agentes donde la calidad de una fuente se mide de acuerdo con el modelo de confianza REGRET. En este modelo, los agentes representan tanto a los usuarios como a las distintas funcionalidades que se presumen del sistema. El diseño sigue la Metodología INGENIAS [22] y fue realizado con las herramientas de que dispone dicha metodología.

Capítulo 4. Se describen las conclusiones extraídas, trabajos futuros y se dan algunas evaluaciones del uso de la Metodología y las Herramientas de INGENIAS en el modelado de la confianza y la reputación en los Sistemas Multiagentes.

Capítulo 2

El Sistema de Vigilancia Tecnológica

Este capítulo presenta formalmente qué es un Sistema de Vigilancia Tecnológica, que está íntimamente asociado a la disciplina de Inteligencia Competitiva. Como ilustración de lo que se espera de estos sistemas, el capítulo incluye un ejemplo de Informe de Vigilancia Tecnológica, que son elaborados por operadores humanos con el soporte de los sistemas que centran este trabajo.

En esta presentación se hace incapié en las dificultades de gestionar fuentes de información, concretamente, al reto de determinar si una fuente es de calidad. Como solución a este problema, se propone la utilización de modelos de confianza. Una selección de estos modelos se revisa en este capítulo.

2.1. La Inteligencia Competitiva y la Vigilancia Tecnológica

Antes de comenzar, conviene aclarar qué es la Vigilancia en el contexto empresarial:

> El esfuerzo sistemático y organizado por la empresa de observación, captación, análisis, difusión precisa y recuperación de información sobre los hechos del entorno económico, tecnológico, social o comercial, relevantes para la misma por poder implicar una oportunidad o amenaza para ésta con objeto de poder tomar decisiones con menor riesgo y poder anticiparse a los cambios [19].

Cuando se habla de Vigilancia Tecnológica, se habla de Vigilancia del entorno tecnológico y, en la actualidad, se habla de Vigilancia Tecnológica como un concepto supeditado al de la Inteligencia Competitiva. Ésta se puede ver como:

- La Inteligencia Competitiva es la obtención ética y legal, análisis y distribución de la información sobre el entorno competitivo, incluyendo los puntos fuertes y débiles así como las intenciones de los competidores [6].

- La Inteligencia Competitiva es el proceso a través del cual las organizaciones obtienen informaciones útiles sobre sus competidores que utilizan en sus planes a corto y largo plazo [9].

En la primera definición se describe el proceso y la información que se maneja. En la segunda definición se describe el resultado y el objetivo final del proceso. Se puede decir que una definición completa la otra.

Algunos autores sostienen que este último tiene un carácter más global[7][1]. Algunos incluso especifican que la diferencia radica en que la Inteligencia Competitiva tiene una dimensión económica que la Vigilancia Tecnológica no tiene [1].

En general, la Vigilancia Tecnológica se asocia más con la observación y análisis de la información para convertir señales dispersas en tendencias y recomendaciones para la organización [4]. En cambio, la Inteligencia Competitiva añade una orientación al uso estratégico de la información analizada. Es decir, la Inteligencia Competitiva es la acción de definir estrategias en la organización partiendo del resultado de las acciones de la Vigilancia Tecnológica y otras informaciones (como es la misma visión de la organización) [12].

Para la realización de la Vigilancia Tecnológica se necesita de todo un conjunto de procesos los cuales constituyen el Sistema de Vigilancia Tecnológica. En la sección 2.2 se hace una definición conceptual de este sistema y de los proceso que contiene.

2.2. Definición de Sistema de Vigilancia Tecnológica

La Vigilancia Tecnológica tiene diversas acepciones:

- La Vigilancia Tecnológica es un proceso organizado, selectivo y permanente, de captar información del exterior y de la propia organización sobre ciencia y tecnología, seleccionarla, analizarla, difundirla y comunicarla, para convertirla en conocimiento para tomar decisiones con menor riesgo y poder anticiparse a los cambios [4].

- La Vigilancia Tecnológica es el arte de descubrir, recolectar, tratar, almacenar informaciones y señales pertinentes, débiles y fuertes, que permitirán orientar el futuro, y proteger el presente y el futuro de los ataques de la competencia. Transfiere conocimientos del exterior al interior de la empresa [27].

- La Vigilancia Tecnológica es la observación y el análisis del entorno seguidos por la difusión bien especificada de las informaciones seleccionadas y analizadas, útiles para la toma de decisiones estratégicas [14].

- La Vigilancia Tecnológica es una forma sistemática de captación y análisis de información científico-tecnológica que sirve de apoyo en los procesos de toma de decisiones [2].

En todos los casos, se puede identificar unos proceso de observación del entorno tecnológico para extraer conocimiento. Esto incluye obtención, análisis y difusión

de información de innovación, investigación y desarrollo tecnológico exterior para el interior de la organización.

Finalmente, se define Sistema de Vigilancia Tecnológica como el conjunto de procesos que tiene como fin hacer la Vigilancia Tecnológica.

La diferencia entre el espionaje y la Vigilancia Tecnológica radica en el aspecto legal y ético de la obtención y tratamiento de la información [4][8]. Estos aspectos hay que tenerlos en cuenta durante todo los proceso de un Sistema de Vigilancia Tecnológica.

El objetivo principal de los procesos de Vigilancia Tecnológica es convertir información en conocimiento para la organización. Conocimiento para ser utilizado en los ajustes de proyectos, estrategias, entre otros. Este conocimiento se refleja en informes que describen las tendencias y cambios significativos para la organización, los cuales se denominan: Informes de Vigilancia Tecnológica. Ejemplos de estos informes son:

- Tecnologías software orientadas a servicios [12]
- Servicios y tecnologías de teleasistencia: tendencias y retos en el hogar digital [3]
- Gestión térmica de sistemas espaciales [26]

En la figura 2.1 se resumen los procesos de un Sistema de Vigilancia Tecnológica que se describen a continuación en las siguientes secciones [1].En este trabajo el proceso de Sistema de Vigilancia Tecnológica va constar de tres fases. En la figura 2.1 se identifican tres:

1. Los pasos previos: la identificación de necesidades y fuentes de información.
2. El procesado de las fuentes.
3. El análisis de las fuentes para la generación del Informe de Vigilancia Tecnológica.

Estas fases se describen a continuación, usando como base el esquema de la figura 2.1.

2.2.1. Pasos previos a la vigilancia

La primera parte consiste en la *identificación de las necesidades de información* de la organización. Esto esta condicionado por los temas de interés de la organización, así como también por sus estrategias internas [4][8].

Una vez que se identifica el «qué» es lo que se necesita. Se procede a buscar e *identificar fuentes de información* donde realizar la vigilancia. Estas fuentes pueden ser

[1]Las siguientes secciones están sobre todo basadas en la norma UNE 166006:2006 EX [4], ya que el hecho de que exista una norma que defina el Sistema de Vigilancia Tecnológica hace que esta se convierta en la principal referencia de información. Sin embargo, también se hacen referencias a otros trabajos para completar información y/o para contrastar.

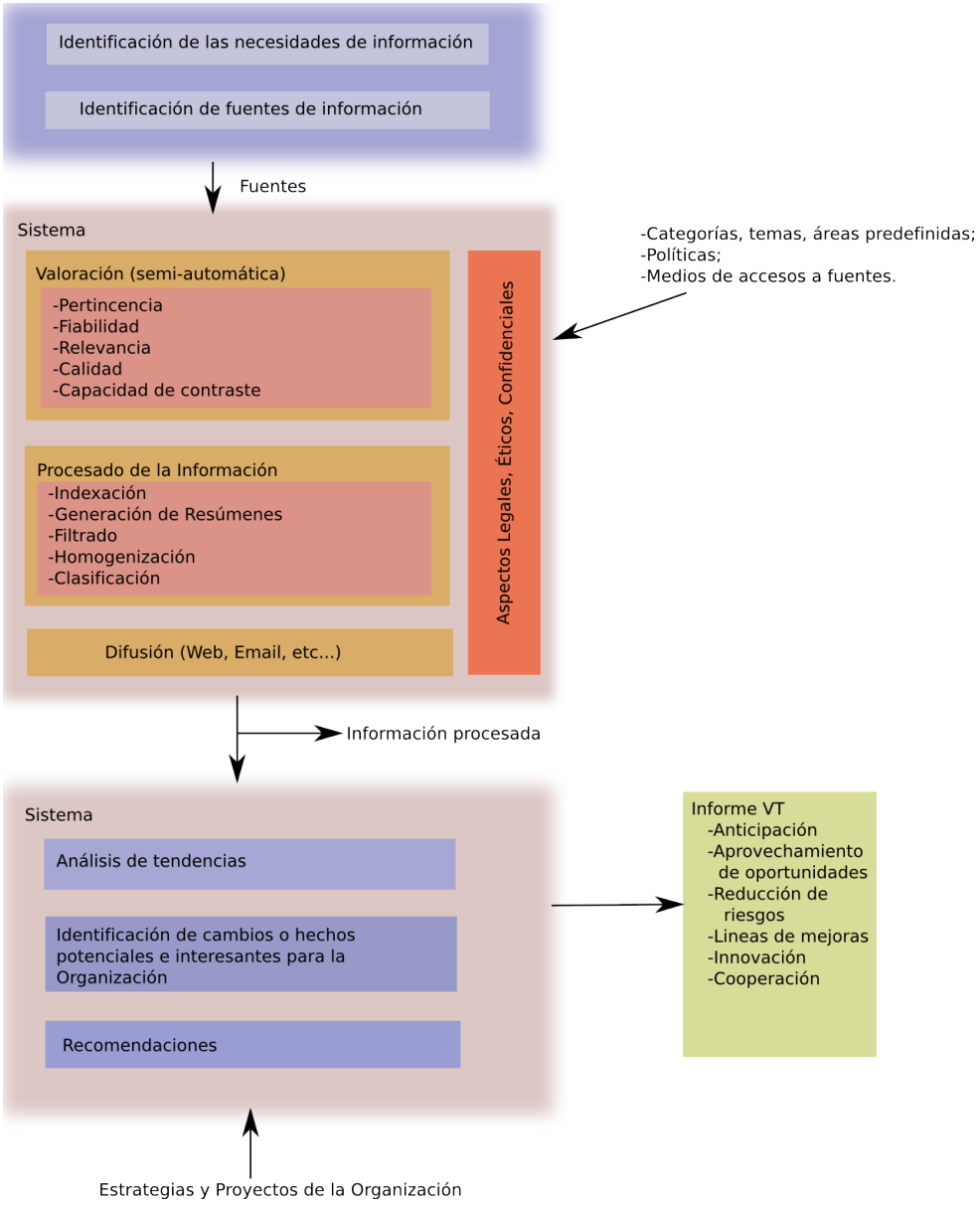


Figura 2.1: Resumen gráfico de los procesos de un Sistema de Vigilancia Tecnológica

bases de datos de patentes, publicaciones científicas, informes técnicos, repositorios de información de proyectos, entre otros [4][8].

En este trabajo se habla de **fuentes de información** como un:

- Localizador de un Documento con Información,
- Localizador de una Lista de Referencias a otras fuentes de información [2],
- Localizador de un Documento con Información y que a su vez tiene Referencias a otras fuentes de información.

Se habla de **documento** como un recurso accesible y procesable con información científico-técnica.

En una organización dedicada a I+D los clientes de un Sistema de Vigilancia Tecnológica son sobre todo los mismos grupos de investigación. Estos investigadores en muchos casos tiene las fuentes de información de interés ya localizadas. Debido a esto los investigadores son un grupo potencial de usuarios proveedores de fuentes de información. Si el sistema se llenara de fuentes de mala calidad, los resultados, y por tanto, los análisis saldrían con mucho ruido y dando señales que pueden ser erróneas debido a estos mismos ruidos. Esto plantea la necesidad de que el sistema sea capaz de filtrar las propuestas de los investigadores. Los investigadores que dedican mucho tiempo a seleccionar las fuentes según ciertos criterios, tienen mayor probabilidad de introducir fuentes con buena calidad. En cambio, los investigadores que dedican poco tiempo a evaluar las fuentes, tienen mayor probabilidad de introducir fuentes de mala calidad.

Una vez determinados los filtros por lo que deben pasar las propuestas, por cuestiones de optimización, debe haber algún control de selección del conjunto de filtros a aplicar, pues de los investigadores que suelen introducir fuentes de calidad se puede esperar que sigan introduciendo fuentes de calidad en el futuro.

Tenga en cuenta que el filtro del que se habla aquí es para aplicar *antes* de que la fuente pase a ser vigilada. Es un filtrado sobre las propuestas de fuentes. También existe otro tipo de filtrado pero es para se aplicado *después* que la fuente haya sido introducida y este en proceso de vigilancia. En este último caso, el filtrado sería para eliminar fuentes de mala calidad que están introduciendo ruido en los resultados. Ambos tipos de filtrado tienen como objetivo mantener al sistema libre de fuentes ruidosas.

En los trabajos consultados se habla de filtrar las fuentes como un paso posterior a la identificación. Pero cuando se orienta a la automatización del Sistema de Vigilancia Tecnológica se identifican dos filtrados distintos, que son los mencionados anteriormente.

Existen técnicas de «confianza» y «reputación» en los agentes inteligentes que resultan adecuadas aplicar para este problema. Técnicas de este tipo facilitarían la toma de decisiones de selección del conjunto de filtros a aplicar en cada caso.

[2] Se pudiera ver este caso como una especialización del siguiente. Pero desde el punto de vista de las propuestas de fuentes por investigadores en un ámbito Web no es lo mismo que se proponga al sistema una lista de referencias de fuentes interesantes que un documento HTML que tenga por «accidente» referencias a fuentes de información no pertinentes (e.g. publicidad). Véase la sección 2.4 para más información.

2.2.2. El procesado de la información

Una vez que se identifican las fuentes de información se procede a introducirlas en el sistema para ser «vigiladas». Esto es, recuperar la información que contienen, procesarla y prepararla para ser analizada; todo esto de manera sistemática para detectar cambios y tendencias globales [4][8]. Estos cambios pueden ser, por ejemplo, organizaciones que comienzan a publicar sobre temas que antes no publicaban, y las tendencias pueden ser el aumento de publicaciones de un determinado tema con el tiempo.

Para la valoración de las fuentes de manera semi-automática hace falta un procesado mínimo que permita asignar ciertos valores a atributos de valoración de la fuente. Hay atributos de valoración que son subjetivos y asignables únicamente por usuarios de la información como «claridad», esto implica que dicha fuente ha de ser procesada y difundida a un grupo de usuarios para poder ser valorada.

Concretamente, en la norma UNE 166006:2006 EX[4] se dan un conjunto de atributos de valoración para las fuentes: pertinencia, fiabilidad, relevancia, calidad y capacidad de contraste. En el libro de Escorsa *et al*[8] se habla de evaluar según su validez (digna de fe, digna de fe pero con riesgos de error o de subjetividad, poco segura,y sospechosa) y según el tamizado (importante, interesante, útil para la ocasión, e inútil). La norma menciona criterios de valoración pero carecen de una completa definición, y en el trabajo de Escorsa *et al*[8] no se abarcan todos los aspectos valorables de una fuente de información. En la sección 2.4 se propone un sistema de valoración alternativo y se hace un análisis de este proceso.

En la norma UNE 166006:2006 EX[4] se indica que la información durante el procesado ha de ser:

Filtrada. Se realiza una valoración de las fuentes con el fin de identificar las fuentes que producen ruido y eliminarlas de los resultados.

Homogeneizada. Estructurar la meta-información de todos los documentos de la misma manera. Por ejemplo, que todos los documentos tenga un campo «título», «contenido», «palabras claves», «fecha de creación», «autores», «institución», entre otros.

Clasificada. Clasificar documentos según sus contenidos. En la norma no se menciona si estas clases han de estar predefinidas o no. La clasificación está sujeta a las necesidades de la organización cliente del Sistema de Vigilancia Tecnológica.

Para la clasificación y análisis textual en general hay técnicas disponibles.

El trabajo de Feldman *et al* [10] es una de las propuestas más citadas. El trabajo plantea la detección de cambios y tendencias a partir del siguiente mecanismo:

1. Se etiquetan los documentos mediante técnicas de *pattern matching*. Las etiquetas están en forma jerárquica y describen conceptos. Subir en la jerarquía significa llegar a conceptos más generales. Se trata etiquetar los documentos con los conceptos más altos en la jerarquía.

2. La detección de cambios y tendencias se realiza mediante el cálculo de las diferencias entre las distribución de etiquetas de un etiquetado antiguo y uno actual.

En el trabajo de Papka *et al* [20] el enfoque es distinto. Las clases están definidas mediantes «consultas». Los documentos se clasifican calculando la similitud con todas las «consultas» de las clases, y donde hay mayor similitud allí se clasifica el documento. Hay un proceso previo de aprendizaje y detección de clases basado en las técnicas de *self-organizing maps*.

Los cambios y tendencias se detectan analizando la evolución en el tiempo del número de documentos de cada clase.

En el trabajo de Rajaraman *et al* [23] presentan un sistema basado en Redes Neuronales para clasificar documentos representados como vectores. Primeramente se realiza un proceso de aprendizaje de las redes con conjuntos de entrenamiento. Finalmente la clasificación se realiza usando dichas redes entrenadas.

Los cambios y las tendencias se detectan analizando la evolución en el tiempo del número de documentos de cada clase.

Toda esta información procesada ha de ser difundida para los usuarios del Sistema de alguna forma [4][8]. Una de las formas más utilizadas para este fin es la difusión vía Web para realizar consultas y Correo electrónico como medios de comunicación de alertas, envíos de informes, entre otros.

2.2.3. El Informe de Vigilancia Tecnológica

El Sistema de Vigilancia Tecnológica tiene como resultado final un Informe donde presenta el resultado del análisis de la vigilancia.

El contenido de este informe debe ser una síntesis del estado actual de las tecnologías y aspectos relacionados que interesan a la organización. Además, debe contener documentado el análisis de dicha síntesis [8], es decir:

- identificadas las nuevas oportunidades,
- identificadas las amenazas,
- descrita las propuestas de decisiones anticipatorias.

En el cuadro 2.1 se describe el contenido específico que debe tener un Informe de Vigilancia Tecnológica según la norma UNE 166006:2006 EX[4].

Para dar una visión más clara del contenido de un Informe de Vigilancia Tecnológica se realiza un descripción del contenido del informe de Vigilancia Tecnológica «Tecnologías software orientadas a servicios» publicado en el 2008 en `madri+d` [12]:

A continuación se describen algunos de capítulos de dicho informe.

Capítulo 2. *Contexto económico y social del sector software* Este capítulo tiene como objetivo contextualizar el software y los servicios en un entorno empresarial tanto en España como en Europa.

Contenido	Descripción
Anticipación	Propuestas de decisiones anticipatorias
Aprovechamiento de oportunidades	Identificación de nuevas oportunidades para la organización
Reducción de riesgos	Identificación y análisis de amenazas para la organización
Líneas de mejoras	Mejoras para superar desfaces y minimizar debilidades en los proyectos de la organización
Innovación	Propuestas de ideas y nuevos proyectos en base al análisis realizado
Cooperación	Identificación de colaboradores potenciales

Cuadro 2.1: Contenido de un Informe de Vigilancia Tecnológica según la norma UNE 166006:2006 EX

Se utiliza para ello datos económicos como indicadores de la importancia y del crecimiento del sector software tanto en el mercado como en la investigación, desarrollo e innovación.

También se utilizan datos estadísticos temporales para indicar dicha importancia y crecimiento. Algunos datos estadísticos son: crecimiento del número de artículos en wikipedia, crecimiento del volumen de contenidos generados por usuarios, crecimiento del número de blogs, entre otros.

Estos últimos datos son muy específicos del tema del informe. Un sistema software de Vigilancia Tecnológica puede tener los datos para generar informes estadísticos específicos del dominio.

Capítulo 3. *Tecnologías existentes.* En este capítulo se introducen conceptos básicos para establecer la relación entre software y servicio.

Capítulo 4. *Estudio de Vigilancia Tecnológica: tendencias de I+D en el ámbito del software orientado a servicios.* En este capítulo se hace un análisis de las tendencias en I+D+i del software orientado a servicio.

Para realizar este análisis se recogen datos estadísticos de las tendencias en publicaciones científicas, patentes, proyectos y grupos I+D.

En esta parte está la principal utilidad final de las herramientas de Vigilancia Tecnológica. Las funciones de consultas y de generación de informes para el análisis serían las piezas claves para este capítulo del Informe de Vigilancia Tecnológica.

Capítulo 5. *Oportunidades tecnológicas y de negocio: factores de éxito.* En este capítulo se hace un análisis de las oportunidades de investigación y explotación que hay en el sector software orientado a servicios.

Capítulo 6. *Propuestas de actuación y recomendaciones* Finalmente en este capítulo se realiza un estudio sobre recomendaciones y riesgos de la adopción de la tecnología presentada en el informe.

Un sistema software si bien no produce automáticamente dicho informe, al menos debe dar soporte a la construcción de dicho informe. Este soporte puede ser el análisis textual y estadístico de las tendencias y los cambios en las fuentes de información anteriormente dadas.

En el Informe de Vigilancia Tecnológica presentado anteriormente (entre muchos otros) se puede apreciar una enorme cantidad de gráficos y tablas con datos estadísticos. Algunos de estos se enumeran a continuación:

- Evolución del número de publicaciones en el período 2000-2006
- Ranking de autores con más publicaciones en la línea especificada
- Instituciones que más publicaciones acreditan
- Países de origen de las publicaciones
- Evolución de la publicación científica por países
- Categorías de investigación de las publicaciones
- Evolución de la solicitud de patentes
- Organismos solicitantes de patentes
- Principales investigadores-titulares de patentes

En este trabajo, las tareas que generan estos gráficos a partir de los análisis textuales se les llama funciones de análisis textual.

El conjunto total de funciones de análisis textual no es algo predefinido a priori, ya que cada organización puede tener necesidades específicas, incluso para cada tipo de informe. La variedad de gráficos y tablas es indeterminado.

Cada función tiene objetivos distintos, incluso las funciones con objetivos similares pueden usar internamente técnicas distintas para obtener los resultados.

A esto se añade que todas estas funciones usan recursos computacionales intensivamente y de manera competitiva.

El sistema software debe dar la posibilidad de introducir funciones de este tipo de manera incremental y dinámica, y también gestionar las mismas para facilitar la reutilización de cómputo y planificar el uso de recursos computacionales.

También se ha visto que hay distintas técnicas de clasificación de texto. Además de esto, las variantes posibles de taxonomías de clasificación es indeterminada. Se pudiera necesitar, por ejemplo, que se genere un gráfico de número de publicaciones por autor clasificados por temáticas. Una tarea de análisis textual puede reutilizar la clasificación hecha previamente por otra tarea de análisis textual que tenía otros objetivos. Esto refleja la utilidad de reutilizar resultados intermedios y finales entre tareas de análisis textual para optimizar el uso de recursos computacionales.

Para este tipo de problema, existen técnicas de agentes inteligentes relacionadas con la cooperación y coordinación para la ejecución de planes distribuidos. Llamando «planes» a las tareas de análisis textual ejecutadas en cierto orden para optimizar el uso de recursos al máximo y obtener resultados lo antes posible.

2.3. Aportaciones del enfoque de agentes al desarrollo de un Sistema de Vigilancia Tecnológica

Los Sistemas de Vigilancia Tecnológica son principalmente sistemas de gestión de información.

El uso exitoso de agentes inteligente para la gestión de la información, así como para su recuperación y tratamiento ha sido demostrado en sistemas reales como Amalthea, CiteSeer, InfoSpider, AIR, entre otros [15][16][5].

Estos sistemas han planteado su arquitectura basada en agentes inteligentes. Dichos agentes son «entidades» software con cierto grado de autonomía en decisiones, con responsabilidades y objetivos a cumplir, incluso algunos con cierta capacidad de movilidad (transporte de código y datos lógicamente tratado como un «agente»). Algunos de los tipos de agentes son: agentes de búsqueda, agentes de filtrado, agentes de monitorización, entre otros.

Uno de los temas interesante donde el uso de técnicas de agentes inteligentes también es clave es en la selección de conjuntos de filtros mediante técnicas de «confianza» y «reputación». Se quiere que el sistema sea capaz de modelar y calcular el nivel de confianza que tiene en un investigador y así poder predecir la calidad de las propuestas futura tiene mucha utilidad a la hora de optimizar el proceso de filtrado. En la sección 2.4 se realiza un estudio de la aplicación de estas técnicas en el Sistema de Vigilancia Tecnológica.

2.4. La Valoración, la Confianza y el Filtrado

Como se ha indicado anteriormente, parte del proceso de vigilancia implica la introducción de fuentes de información en el sistema para ser vigilados (ver la figura 2.1). La norma misma indica que estas fuentes debe ser valoradas según ciertos criterios y filtradas para eliminar ruidos y falsas señales.

Hay dos tipos de filtrado en éste tipo de sistemas. El primero de ellos se refiere a las fuentes de mala calidad que ya han sido introducidas y aceptadas en el sistema y están generando ruido. El filtrado aquí consiste en eliminar estas fuentes para que dejen de afectar los resultados de los análisis.

El segundo de ellos se refiere a filtrar las fuentes propuestas por los investigadores para prevenir la presencia de fuentes de mala calidad en el sistema. Este tipo de filtrado es al que se refiere el resto de este trabajo.

En el sistema, debe existir un mecanismo de valoración para luego utilizarlo en el filtrado de fuentes.

El sistema tiene que realizar una valoración de las fuentes propuestas antes de aceptarlas para la vigilancia. El cálculo de estos valores resulta costoso y lento. Hay valores que requieren interacción con expertos, otros que requieren realizar consultas ficticias, etc. (ver la sección 2.4.1).

El uso de modelos de confianza y reputación para predecir la valoración de una fuente recién propuesta por un investigador resulta útil para seleccionar el conjunto de filtros a aplicar. Llamándose filtro como la acción de valorar la fuente en un

aspecto concreto y decidir si pasa la fuente o no en función de dicha valoración. La idea es que si un investigador suele introducir fuentes que son valoradas en unos criterios como buena pero en otros como regular o mala, el sistema solo necesita aplicar filtro para los criterios con problemas.

En las secciones siguientes se explica estos asuntos con mayor exactitud.

2.4.1. Métodos y Criterios de Valoración

Antes que nada, se necesita un sistema de valoración de fuentes de información lo más completo y práctico posible. En la norma [4] se mencionan algunos criterios de valoración pero carece de una completa definición de las mismas, y en [8] no se abarcan todos los aspectos valorables de una fuente de información. En este trabajo se ha estudiado sobre todo el trabajo de Naumann *et al* [18] como un completo sistema de valoración a aplicar. En [18] se hace una recopilación de varios criterios existentes y se unifican creando un nuevo método con un conjunto de criterios bien esquematizados y definidos.

Naumann *et al* definen tres conjuntos de criterios (atributos) de valoración [3].

Subject-criteria. Criterios más bien subjetivos como «claridad», «valor añadido», entre otros. La fuente principal de esta información es el usuario.

Process-criteria. Criterios del procesado como son «tiempo de respuesta», «latencia», «disponibilidad», entre otros. Esta información se obtiene durante la ejecución de las consultas sobre las fuentes de información.

Object-criteria. Criterios de la fuente en sí, por ejemplo, «completitud», «precio», «antigüedad», entre otros. Esta información se obtiene de la fuente de información en sí misma.

En el artículo se dan un conjunto completo de criterios y sus significados. En el cuadro 2.4.1 (tomado de [18]) se da una lista completa de cada uno de los componentes de los criterios.

Para dar la valoración se describen un conjunto de métodos (ver figura 2.2 como resumen). Para los «Subject-criteria» recomiendan sobre todo el uso de encuestas a los usuarios. Para los «Process-criteria» se recomienda que durante el proceso de consulta se midan todo estos criterios. Finalmente para los «Object-criteria» se recomienda asignar algunos valores automáticamente por el «parsing» de los metadatos de la fuente de información (si están disponibles y son procesables) y otros mediante el trabajo de expertos.

En dicho trabajo se considera la «fuente de información» como el localizador de un documento con información. En el caso de los Sistemas de Vigilancia Tecnológica, en muchas ocasiones interesa introducir fuentes de información que son más bien listas de referencias a otras fuentes de información. La valoración de una fuente de este tipo debe depender en cierto grado de las valoraciones de las fuentes a las que hace referencia.

[3] Se ha optado por mantener los nombres de las categorías en inglés. La traducción aproximada sería «Criterios subjetivos», «Criterios de procesado» y «Criterios del objeto»

Clase de Criterio	Criterio
Subject-criteria	Credibilidad
	Representación concisa
	Interpretabilidad
	Relevancia
	Reputación
	Claridad
	Valor añadido
Object-criteria	Completitud
	Soporte al Cliente
	Documentación
	Objetividad
	Precio
	Fiabilidad
	Seguridad
	Antigüedad
	Verificabilidad
Process-criteria	Precisión
	Cantidad de Datos
	Disponibilidad
	Coherencia de la Representación
	Latencia
	Tiempo de respuesta

Cuadro 2.2: Criterios IQ

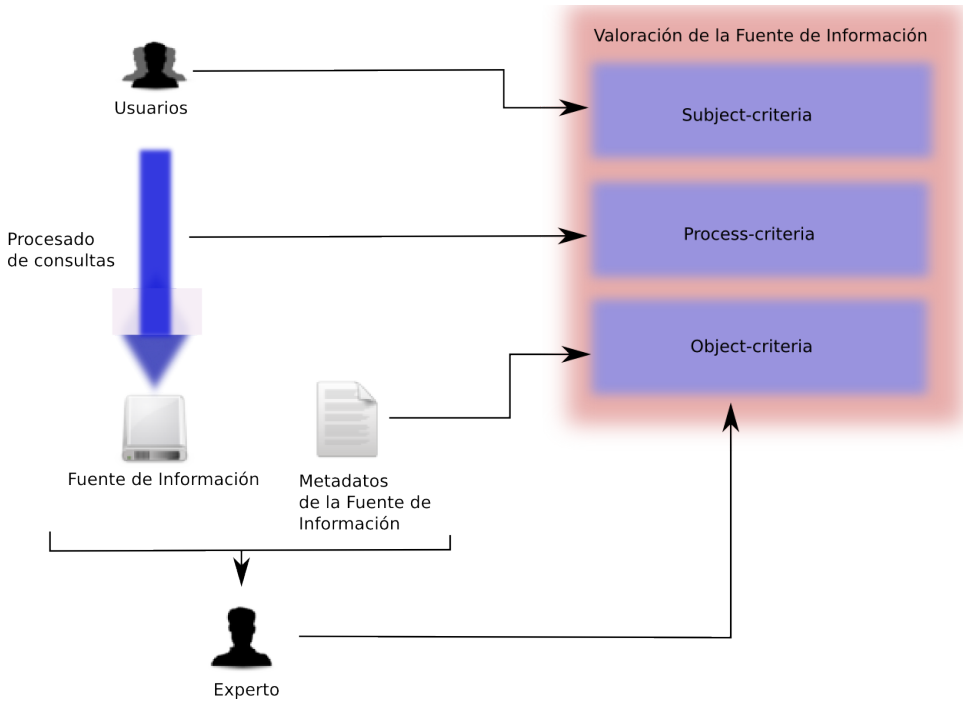


Figura 2.2: Obtención de los valores de los criterios de valoración de fuentes de información

En el trabajo de Nauman *et al* no se estudia este tema, sin embargo es un problema que aparece en los Sistemas de Vigilancia Tecnológica.

Otro aspecto muy importante a tener en cuenta es que en el trabajo de Nauman *et al* los criterios de valoración se miden no teniendo en cuenta siempre el grado de satisfacción. Por ejemplo, «claridad» se mide del 1 al 10 o en porcentajes indicando cuan fácil es entender el texto, pero «tiempo de respuesta» se mide con medidas de tiempo. A la hora de aplicar esto a la «confianza» los criterios a valorar se miden más bien en grado de satisfacción. Al realizar la valoración se suelen utilizar medidas muy sencillas como *malo (-1)*, *neutral(0)* y *bueno(+1)* , por ejemplo «claridad» puede ser −1 (mala) y «tiempo de respuesta» puede ser +1 (bueno); finalmente la valoración final sería el resultado de aplicar una función de agregación a lo anterior.

2.4.2. La Confianza

En la Inteligencia Artificial se define «confianza» según el ámbito en que se usa. Reagle [25] en su tesis categoriza estas definiciones en tres grupos. La categoría más apropiada en el contexto de este trabajo es: *confianza como verdad y creencia*. Más específicamente en el ámbito de este trabajo:

> **confianza** es una *creencia* que tiene un agente respecto al *grado de calidad* de las fuentes de información que otro agente aportador introducirá en el sistema en el *futuro*. Esta confianza esta basada en la *experiencia pasada* con las fuentes introducidas por dicho agente aportador, y en la

reputación que el mismo tiene en la sociedad de agentes en cuanto al grado de calidad que suelen tener las fuentes que propone.

En contraste con la mayoría de los modelos de confianza y reputación en los Sistemas de Vigilancia Tecnológica no es un escenario de e-commerce, aunque si de negociación entre agentes. Más bien en los Sistemas de Vigilancia Tecnológica los Agentes Colaboradores hacen *propuestas* que los Agentes Supervisores del Sistema debe filtrar y luego decidir si *aceptar* o *rechazar* definitivamente. En esta interacción entra en juego los modelos de confianza y reputación para predecir la calidad en cada criterio de la fuente para optimizar el conjunto de filtros a aplicar para decidir si aceptar o rechazar definitivamente una propuesta.

Existen muchos modelos para la «confianza» y la «reputación» en sistemas multiagentes. Algunos modelos son: REGRET [28], RepAge [29], CREDIT [24], FIRE [13] y el trabajo de Mui *et al* [17].

REGRET

REGRET es un sistema modular de confianza y reputación orientado a sociedades complejas de agentes, especialmente en entornos e-commerce. En este sistema, las relaciones sociales entre agentes juegan un papel decisivo.

Partiendo de la experiencia directa, la información de terceras partes (otros agentes) con cierto grado de credibilidad y del conocimiento de la estructura social, el sistema calcula el grado de confianza y reputación que un agente tiene respecto a otro. A todo esto le asigna un grado de fiabilidad basado en la cantidad de información utilizada para calcular el grado de confianza.

En la figura 2.3 (tomada de [28]) se describe gráficamente los módulos del sistema REGRET y sus relaciones de dependencias.

Como se indica en la figura 2.3 el modelo de confianza se basa en lo que en REGRET se le llama *direct trust* y el modelo de reputación. El módulo *direct trust* trata con la experiencia directa del agente y de como esta experiencia afecta al grado de confianza con otros agentes.

El modelo de reputación consta de tres módulos que son usados según la fuente de información de la reputación. Esta fuente de información puede ser un testigo directo (witness reputation), el «vecindario»[4] (neighbourhood reputation) o los roles y propiedades del sistema (system reputation). Para los testigos directos el sistema además tiene un módulo que calcula la credibilidad sobre la información proporcionada de REGRET.

Otro aspecto es el uso de ontologías para expresar la relación de los atributos que constituyen el grado de confianza. El sistema usa dicha ontología a la hora de determinar el grado de confianza general. Un ejemplo ilustrativo es el dado en la tesis[28]: la reputación de ser una buena compañía de vuelos es el resultado de una reputación de tener buenos planes de vuelo, de no perder nunca los equipajes y de servir una buena comida.

[4] Testigos indirectos

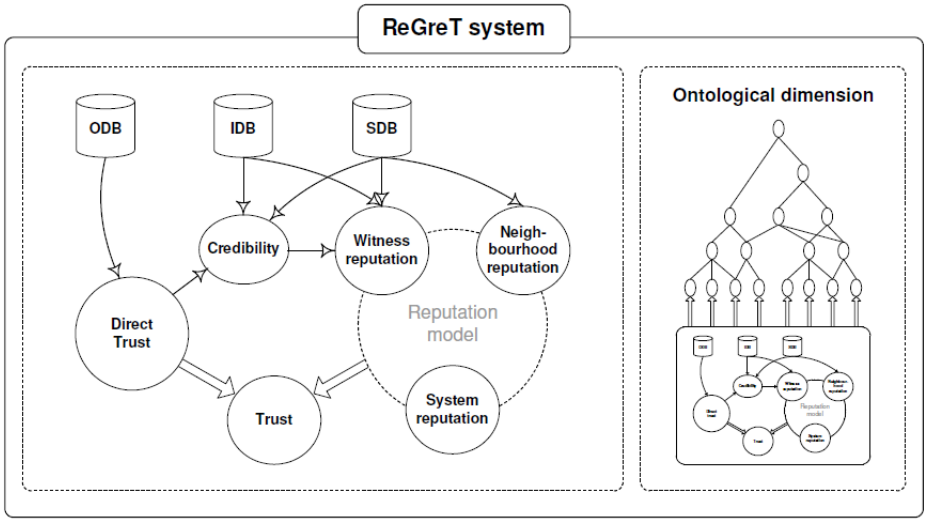


Figura 2.3: Módulos del sistema REGRET

REGRET es un sistema cuyos principios podrían aplicarse en los Sistemas de Vigilancia Tecnológica. El hecho de ser modular permite prescindir de ciertos módulos que no se usan nunca o ciertos módulos que se usan cuando aparece la información necesaria. También el uso de ontologías para los atributos es útil ya que el grado de confianza sobre las propuesta de un investigador no se deriva de un único término.

Aunque REGRET tiene un módulo de credibilidad y calcula la fiabilidad final de un grado de confianza, parte de que el sistema de valoración de las fuentes es fiable. Como se indica en la sección 2.4.1 parte de los criterios de valoración en un Sistema de Vigilancia Tecnológica son asignados por humanos, y por lo tanto la calidad de la valoración depende del tiempo que dicho humano dedique a hacerlo (ver [18]).

REGRET es un modelo de confianza y reputación aplicable para el problema planteado.

RepAge

RepAge [29] es un sistema que basa su modelo en la teoría cognitiva de la reputación. Dicho modelo hace una clara distinción entre lo que llaman *imagen* y *reputación*. *Imagen* lo definen como la propia evaluación que hace un agente de otro basada en una norma o estándar social y *reputación* como una creencia en cuanto a la evaluación basada en el «boca a boca» de la sociedad de agentes. REGRET es una de las principales influencias de RepAge y comparte con este muchas ideas básicas. RepAge le da bastante importancia al proceso interno de cálculo de la confianza y reputación. Incluso RepAge permite hacer meta-razonamiento sobre la información usada para calcular el resultado final de confianza mediantes el uso de predicados.

En principio este sistema es tan aplicable como el REGRET para el modelo preliminar que se hace. La característica que le distingue del REGRET no introduce alguna mejora sustancial en el modelo preliminar. Se tiene la intención de estudiar su aplicación para modelos más completos y complejos.

CREDIT

CREDIT[5] [24] es un sistema computacional de confianza y reputación similar a REGRET. En contraste con este añade la idea de «normas». En los entornos multiagentes hay normas de comportamiento establecidas. Normas a nivel social, de grupo y de instituciones de agentes.

El nivel de confianza de un agente A en otro agente B esta basado en cuanto satisface B la expectación (especificada o no) de A. Las normas describen las expectaciones no especificadas en los contratos. Por ejemplo,

Si $precio > 100$ Y $QoS = 8$ Entonces $antiDoS = 10$

Esto quiere decir que para precios superiores a los 100u y garantía de calidad de servicio de ocho, se espera un servicio de alto nivel (de 10 en la escala de 1 a 10) de *anti denial-of-service*.

En otro aspecto en el cual CREDIT se diferencia de REGERT es en las funciones concretas de `fuzzy set` que se usan para calcular los valores de confianza.

Esta posibilidad de definir normas que describan las expectaciones no especificadas resulta útil en el modelo de filtrado de este trabajo (ver capítulo 3). Aunque para el modelo preliminar definido no se usa esta posibilidad. En concreto, se puede utilizar para determinar los mínimos y evitar fuentes con evaluaciones incoherentes, pero no a nivel del criterio (Subject-criteria, Object-criteria o Process-criteria) sino ya a niveles de sus componentes. Por ejemplo, se pueden definir normas del estilo:

Si *ReputacionDeLaFuente* > +0,6 Entonces *Credibilidad* > +0,7

Para esto ya habría que utilizar las técnicas de ontologías descritas en REGRET para calcular la confianza final partiendo de la confianza en cada uno de los componentes de los criterios.

FIRE

FIRE[6] [13] es un sistema de confianza y reputación pensado para los sistemas multiagentes abiertos, donde los agentes entran y salen del sistema en tiempo de ejecución.

En este tipo de sistema los modelos de confianza y reputación existentes no son aplicables. Las fuentes de información para el cálculo de la confianza como son la experiencia directa, la información de testigos, las reglas y políticas del sistema, entre otros, pueden no dar la suficiente información nunca respecto a un agente concreto que entra y sale del sistema.

[5] Confidence and REputation Defining Interaction-based Trust
[6] FIRE viene de **fi**des («Confianza» en latin) y **re**putación

Ante esta situación, en FIRE se propone una nueva fuente de información que es proveída por el mismo agente. El agente que entra al sistema da un argumento a favor de que confíen en él presentando una Reputación Certificada.

A diferencia de la reputación basada en los testigos directos, el agente colecta referencias de los que han interactuado con él y presenta él mismo la reputación que tiene ante los testigos directos al agente interesado en saber su reputación. Esta información la presenta de manera certificada y segura. Esto es la Reputación Certificada.

FIRE se presenta como un framework que da soporte a todo un mecanismo que maneja las distintas fuentes de información, incluyendo la Reputación Certificada, para el cálculo final del grado de confianza hacia un agente en un entorno multiagente abierto.

Este sistema de confianza y reputación es aplicable en el modelo preliminar propuesto al igual que REGRET. La característica de Reputación Certificada parte de la necesidad de que los agentes sobre los que se calcula grados de confianza entran y salen del sistema. De momento, en el modelo preliminar propuesto los agentes sobre los que se les calcula grados de confianza no entran y salen del sistema. Por lo que no se utilizaría la característica que le distingue de REGRET para el modelo preliminar de este trabajo.

2.5. Conclusiones

Las labores de Vigilancia Tecnológica se soportan con Sistemas de Vigilancia Tecnológica. Estos sistemas, para ofrecer información de calidad, requieren que las propias fuentes de información que gestiona sean de calidad. Una forma de conseguirlo es mediante modelos de confianza. Se han estudiado cuatro modelos de confianza posibles, todos los cuales parece aplicables al problema en cuestión. Como punto de inicio de la investigación, se elige el más difundido, el REGRET, para su incorporación dentro del diseño orientado a agentes que se verá en la siguiente sección.

Capítulo 3

Modelo Preliminar

En este capítulo se describe el modelo preliminar multiagente propuesto para el filtrado de propuestas y su optimización basado en la confianza y la reputación.

Para el desarrollo de este modelo se ha usado las notaciones de INGENIAS [22]. En el Anexo A se da una breve introducción a la Metodología de INGENIAS y sus notaciones.

3.1. Escenarios

Para la realización del modelo, se ha comenzado con la elaboración de cuatro escenarios a nivel de agentes. Estos escenarios tratan diversas situaciones que pueden surgir en un sistema donde se aplican modelos de confianza. En concreto, se trata de estudiar el tratamiento de:

1. una propuesta de fuente de buena calidad realizada por un agente colaborador por primera vez,
2. una propuesta de fuente de mala calidad realizada por un agente colaborador sobre el cual se tiene un grado de confianza bajo,
3. una propuesta de fuente de buena calidad realizada por un agente colaborador sobre el cual se tiene un grado de confianza alto,
4. una propuesta de fuente de mala calidad realizada por un agente colaborador sobre el cual hay una mala reputación por parte de un agente supervisor testigo de muchas propuestas pasadas.

Escenario 1

Agentes: *Colaborador1*, *Supervisor1*, *InspectorPruebas1*, *Inspector1*, *GestorFuentes1*

Situación de partida: El *Colaborador1* nunca ha enviado ninguna propuesta a ningún Supervisor

Escenario: 1. El *Colaborador1* envía una propuesta de buena calidad al *Supervisor1*

2. El *Supervisor1* ve que no tiene ninguna información sobre el *Colaborador1* y solicita una inspección al *InspectorPruebas1*
3. El *InspectorPruebas1* calcula los valores de los atributos de calidad de la propuesta y le envía al *Supervisor1* la respuesta
4. El *Supervisor1* ve que la calidad es buena y le indica al *Colaborador1* que su propuesta ha sido aceptada
5. El *Supervisor1* envía la propuesta al *GestorFuentes1* para ser introducida en el sistema para su vigilancia
6. El *Supervisor1* envía la propuesta al *Inspector1* para que realice una inspección completa y continua de la fuente

Escenario 2

Agentes: *Colaborador1*, *Supervisor1*, *InspectorPruebas1*

Situación de partida: El *Colaborador1* ha propuesto fuentes de mala calidad en el criterio X al *Supervisor1* el cual ha rechazado

Escenario:
1. El *Colaborador1* envía una propuesta de mala calidad en el criterio X al *Supervisor1*
2. El *Supervisor1* ve que este colaborador ha propuesto fuentes de mala calidad en el criterio X en el pasado y solicita una inspección del criterio X al *InspectorPruebas1*
3. El *InspectorPruebas1* calcula el valor del criterio X de la propuesta y le envía al *Supervisor1* la respuesta
4. El *Supervisor1* ve que la calidad es mala y le indica al *Colaborador1* que su propuesta ha sido rechazada

Escenario 3

Agentes: *Colaborador1*, *Supervisor1*, *InspectorPruebas1*

Situación de partida: El *Colaborador1* ha propuesto fuentes de buena calidad al *Supervisor1*

Escenario:
1. El *Colaborador1* envía una propuesta de buena calidad al *Supervisor1*
2. El *Supervisor1* ve que este Colaborador ha propuesto fuentes de buena calidad en el pasado y envía una respuesta de aceptación de la propuesta al *Colaborador1*
3. El *Supervisor1* envía la propuesta al *GestorFuentes1* para ser introducida en el sistema para su vigilancia
4. El *Supervisor1* envía la propuesta al *Inspector1* para que realice una inspección completa y continua de la fuente

Escenario 4

Agentes: *Colaborador1*, *Supervisor1*, *Supervisor2*, *InspectorPruebas1*

Situación de partida: El *Colaborador1* ha enviado una propuesta de calidad que roza los mínimos en el criterio X al *Supervisor1* y ha enviado propuestas de mala calidad en el criterio X al *Supervisor2*. El *Supervisor1* recientemente ha recibido información muy fiable del *Supervisor2* que el *Colaborador1* tiene problemas con la calidad en el criterio X.

Escenario:

1. El *Colaborador1* envía una propuesta de mala calidad en el criterio X al *Supervisor1*
2. El *Supervisor1*, que aunque no tiene suficiente información para prejuzgar al *Colaborador1*, tiene información de reputación muy fiable que le indica que el *Colaborador1* tiene problemas en el criterio X de calidad de las fuentes. Por lo que decide enviar la fuente al *InspectorPruebas1* para su análisis
3. El *InspectorPruebas1* calcula el valor del criterio X de calidad de la propuesta y le envía al *Supervisor1* la respuesta
4. El *Supervisor1* ve que la calidad es mala y le indica al *Colaborador1* que su propuesta ha sido rechazada

Interacciones identificadas

Las interacciones que se han identificado en estos escenarios son las siguientes:

- Envío de propuestas entre un Agente Colaborador y un Agente Supervisor. Acto del habla: `Proposal`
- Petición de inspeccionar fuentes entre un Agente Supervisor y un Agente Inspector. Acto del habla: `Request`
- Petición de inspeccionar fuentes entre un Agente Supervisor y un Agente Inspector de Pruebas. Acto del habla: `Request`
- Petición de introducir fuentes en el sistema para ser vigiladas entre un Agente Supervisor y un Agente Gestor de Fuentes. Acto del habla: `Request`
- Consulta de reputación entre un Agente Supervisor y el resto de Agentes Supervisores. Acto del habla: `Query`

Estas interacciones se han definido completamente en la sección 3.4.

Las estructura organizativa

La organización de los agentes identificada es la siguiente:

- Hay un grupo de agentes supervisores que controlan la aceptación de propuestas e intercambian información de reputación entre sí. A este grupo pertenecen los agentes *Supervisor1* y *Supervisor2* del escenario.
- Hay otro grupo de agentes colaboradores que proponen fuentes a los supervisores. A este grupo pertenece el agente *Colaborador1* del escenario.
- Hay un grupo de agentes encargados de procesar las fuentes que se van a probar para calcular sus grados de calidad sin ser introducidas en el sistema de vigilancia. A este grupo pertenece el agente *InspectorPruebas1* del escenario.
- Y también hay un grupo de agentes encargados de gestionar las fuentes que son introducidas para su vigilancia. A este grupo pertenecen los agentes *GestorFuentes1* e *Inspector1*.

Esta estructura organizativa se describe en más detalles en la sección 3.2.

El control de filtrado por los Agentes Supervisores

El control del filtrado que tienen los Agentes Supervisores está basado en un modelo de confianza y reputación. La confianza indica que un Colaborador determinado suele proponer fuentes de una determinada calidad.

Esta información del grado de confianza se calcula a partir de la experiencia directa y de la información de reputación de los demás Supervisores.

A esto se le añade un grado de fiabilidad que depende de la cantidad de información que se posee para calcular dicho grado de confianza.

Las decisiones respecto al filtrado dependen finalmente de dicho grado de confianza. Cuando el grado de confianza es bajo en determinados aspectos de calidad, se decide pasar la fuente a un estado de pruebas para calcular los grados de calidad que suelen ser problemáticos en el Colaborador, para luego decidir si pasar la fuente o no. Pero si el grado de confianza es bueno en todos los aspectos entonces se decide aceptar inmediatamente la propuesta.

Que una propuesta haya sido aceptada no quiere decir que se abandone el cálculo de los grados de calidad de la misma, sino que éste cálculo se hace a posteriori a medida que se va realizando la vigilancia de la fuente y los usuarios y expertos la van valorando. Una vez que se tienen los grados de calidad de la fuente actualizados, se le informa al Supervisor, que la aceptó, para que actualice su información de confianza en el Colaborador que la propuso.

En la sección 3.5 se detalla este modelo de control.

3.2. Modelo de Organización de Agentes

Como se puede apreciar en la figura 3.1 la organización de agentes [1] se divide en cuatro grupos lógicos de agentes.

[1] Esta organización esta mostrada parcialmente pues es solo un modelo que implementa las características dichas

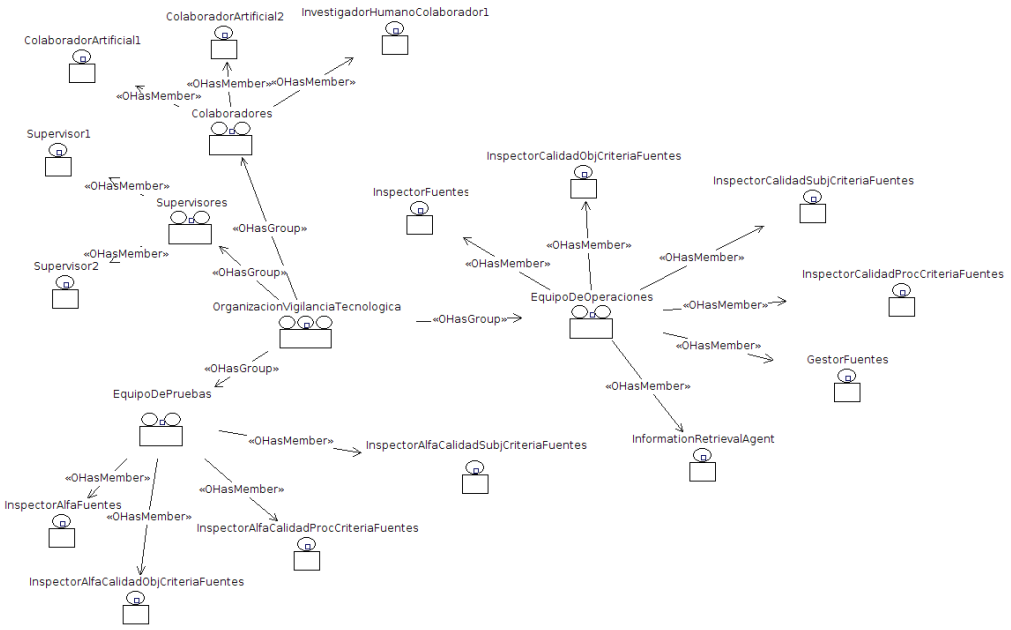


Figura 3.1: Modelo de Organización de Agente para el filtrado de propuestas en el Sistema de Vigilancia Tecnológica

Colaboradores. Agrupa lógicamente a todos los agentes que colaboran proponiendo fuentes. Dichos agentes pueden ser agentes representantes de humanos, o agentes con iniciativas propias para proponer fuentes.

Supervisores. Agrupa lógicamente a todos los agentes que supervisan las propuestas de los colaboradores. Estos agentes son los que finalmente deciden que tipo de filtros aplicar a las propuestas.

Equipo de Pruebas. Agrupa lógicamente a los agentes que se encargan de dar unos grados de calidad a una fuente dada sin ser introducida en el sistema. Para ello pueden utilizar la información de la fuente en si, pueden realizar procesos de consultas ficticias a la fuente y pueden solicitar valoraciones de expertos humanos mediante encuestas.

Equipo de Operaciones. Agrupa lógicamente a los agentes que se encargan de vigilar las fuentes aceptadas y dar el resto de servicios. Aquí se incluyen los agentes encargados de inspeccionar las fuentes aceptadas para mantener actualizada la información de la calidad de las mismas para su uso en el cálculo del grado de confianza en los colaboradores.

3.3. Modelos de Agentes

A continuación se describen los modelos de roles y agentes más relevantes que implementan la característica de filtrado de propuestas de fuentes del sistema, con

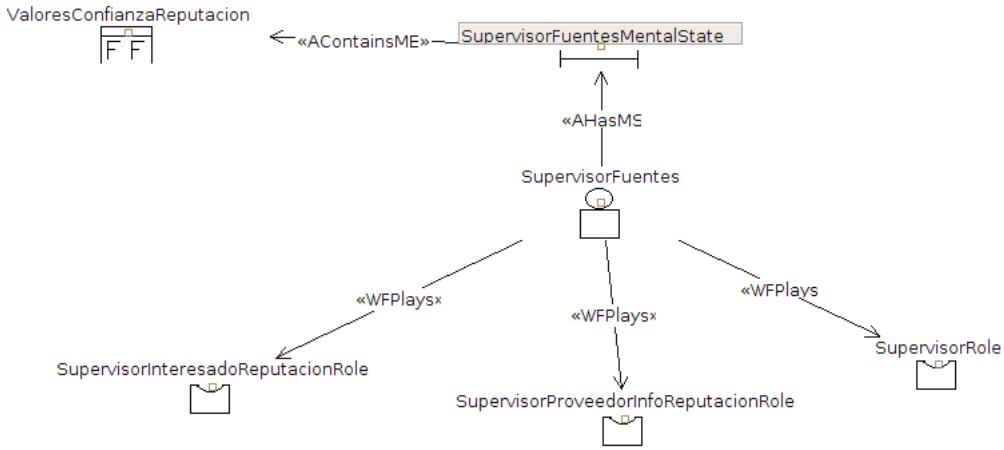


Figura 3.2: Modelo del Agente: Supervisor de Fuentes

las técnicas de confianza y reputación.

3.3.1. El Agente: Supervisor de Fuentes

Como se muestra en la figura 3.2 el agente «SupervisorFuentes» juega en el sistema tres roles que se describen en la siguientes secciones. Estos roles son «SupervisorInteresadoReputacionRole», «SupervisorProveedorInfoReputacionRole» y «SupervisorRole».

El estado mental de éste agente contiene un hecho que almacena los valores del grado de confianza de los agentes colaboradores (ver detalles en 3.3.5) que le han propuesto fuentes.

3.3.2. El Rol: Supervisor

En la figura 3.3 se describen las capacidades del rol «SupervisorRole». Este rol tiene como objetivo *mantener el sistema con fuentes de buena calidad*.

Las capacidades de este rol están expresadas como tareas que puede realizar. Estas tareas están modeladas en las figuras 3.3, 3.4, 3.5, 3.6, 3.7 y 3.8.

Cuando mediante la interacción «PropuestaFuente» (sección 3.4.1) llega una propuesta de fuente al supervisor se lanza la tarea «ProcesarPropuestaRecibidaTask».

Esta tarea se encarga de realizar el control del filtrado (ver sección 3.5). Partiendo del grado de confianza que tiene respecto al agente colaborador que inició la interacción, decide si:

- Rechazar completamente la propuesta pues el agente colaborador hizo suficientes intentos de proponer fuentes de mala calidad [2]. Para ello produce el

[2]El número de intentos es un parámetro a establecer en el sistema. Suele ser suficiente establecer

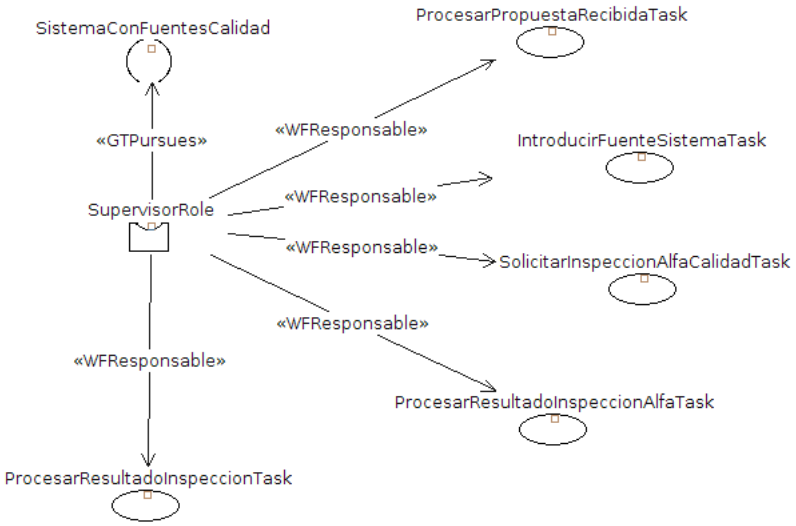


Figura 3.3: Modelo del Rol: Supervisor

hecho «PropuestaRechazada» que es enviado como respuesta en la interacción con el acto del habla `reject-proposal`.

- Solicitar la inspección de la fuente en determinados aspectos al Equipo de Pruebas (ver sección 3.2). Para ello produce el hecho «FuenteParaCuarentena».

- Solicitar la introducción de la fuente en el sistema. Para ello produce el hecho «FuenteParaProcesado».

Además de esto, la tarea produce un hecho del tipo «ReputacionAgenteNecesaria» para indicar que se necesita actualizar la información de reputación del agente colaborador. Este hecho luego provoca la creación de una conversación con el resto de supervisores para actualizar dicha información (ver sección 3.3.3).

En el caso de que se haya solicitado la introducción de la fuente en el sistema. Se activa la ejecución de la tarea «IntroducirFuenteSistemaTask» ante la presencia del hecho «FuenteParaProcesado» (ver figura 3.5).

Esta tarea realiza tres operaciones:

- Solicita una inspección de calidad creando para ello una conversación de «SolicitudInspeccionCalidad» y un hecho «InspeccionarCalidadFuente».

- Pide la introducción de la fuente en el sistema creando para ello una conversación de «PeticionIntroducirFuente» y un hecho «FuenteNueva».

- Responde al agente colaborador que ha propuesto un `acept-proposal` generando para ello el hecho «PropuestaAceptada» que es precondición para el `acept-proposal` de la conversación de «RealizacionPropuesta».

tres intentos como mucho.

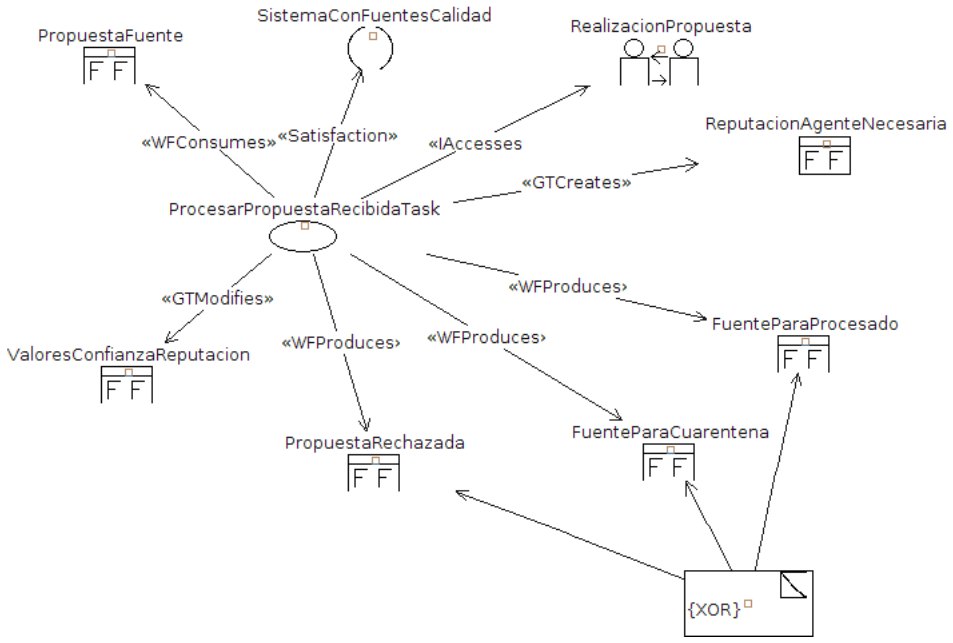


Figura 3.4: Modelo de la Tarea: Procesar Propuesta Recibida

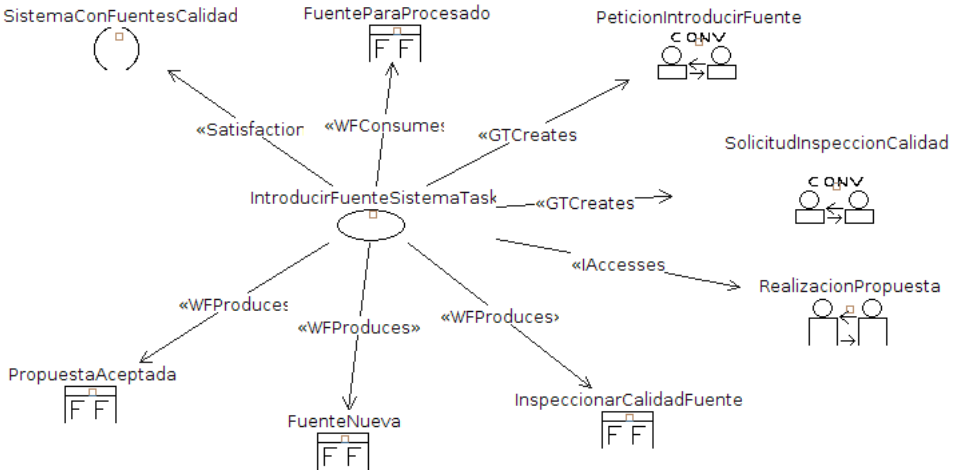


Figura 3.5: Modelo de la Tarea: Introducir Fuente en el Sistema

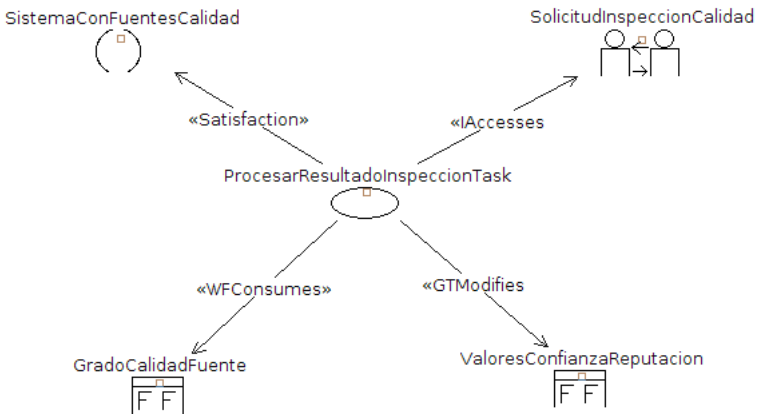


Figura 3.6: Modelo de la Tarea: Procesar Resultado de Inspección

Aunque la conversación con el colaborador termina, la conversación generada para la inspección se mantiene activa y es de larga duración.

Al cabo del tiempo, cuando el inspector de calidad responde se activa la tarea «ProcesarResultadoInspeccionTask» la cual esta descrita en la figura 3.6.

Esta tarea consume el hecho «GradoCalidadFuente» que viene en la respuesta de la conversación y actualiza los valores de confianza de los agentes colaboradores que le han propuesto fuentes.

En el caso de que se solicite obtener y calcular los grados de calidad de ciertos aspectos de la fuente antes de decidir se activa la tarea «SolicitarInspeccionAlfaTask» antes la presencia del hecho «FuenteParaCuarentena». En la figura 3.7 se describe el modelo de la tarea.

Esta tarea realiza la operación de solicitar la inspección de calidad, y para ello crea una conversación del tipo «SolicitudInspeccionAlfaCalidad» y genera el hecho «InspeccionarCalidadFuenteCuarentena».

En cuanto llega la respuesta de la solicitud se activa la tarea «ProcesarResultadoInspeccionAlfaTask» ante la presencia del hecho «GradoCalidadFuenteCuarentena». En la figura 3.8 se describe el modelo de la tarea.

Esta tarea tiene tiene dos posibles salidas. La primera de ellas es aceptar finalmente la propuesta generando para ello el hecho «FuenteParaProcesado» o respondiendo con `reject-proposal` mediante la generación del hecho «PropuestaRechazada».

Esta tarea también actualiza el valor de confianza que tiene hacia el agente colaborador con los nuevos datos de calidad recibidos.

3.3.3. El Rol: Supervisor Interesado en Información de Reputación de Agente

El rol «SupervisorInteresadoReputacionRole»(ver figura 3.9) lo juega el agente supervisor cuando esta interesado en conocer la reputación que tiene un agente colaborador en los demás supervisores. Esto tiene como objetivo mantener actualizada

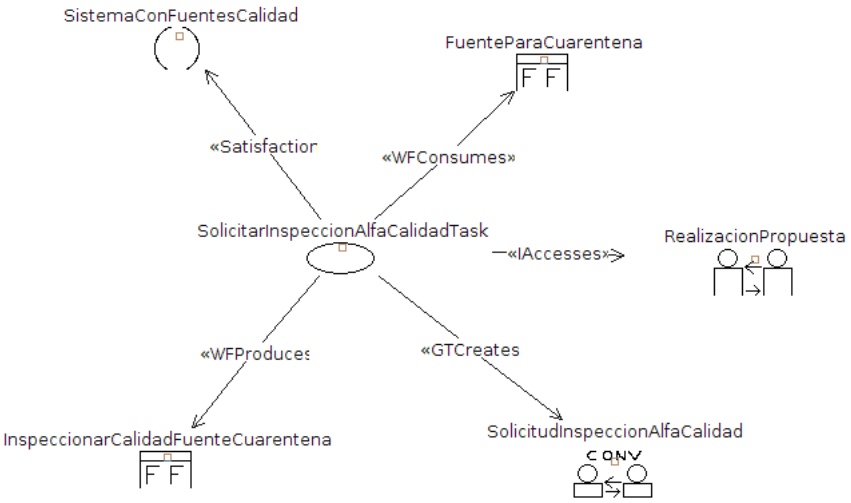


Figura 3.7: Modelo de la Tarea: Solicitar Inspección Alfa de Calidad

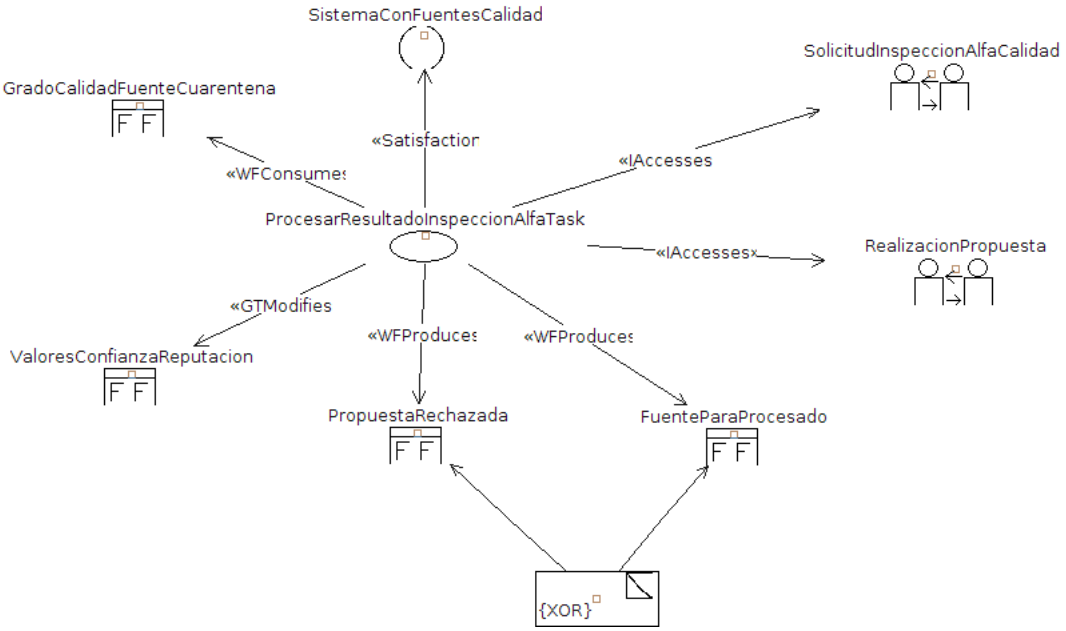


Figura 3.8: Modelo de la Tarea: Procesar Resultado de Inspección Alfa

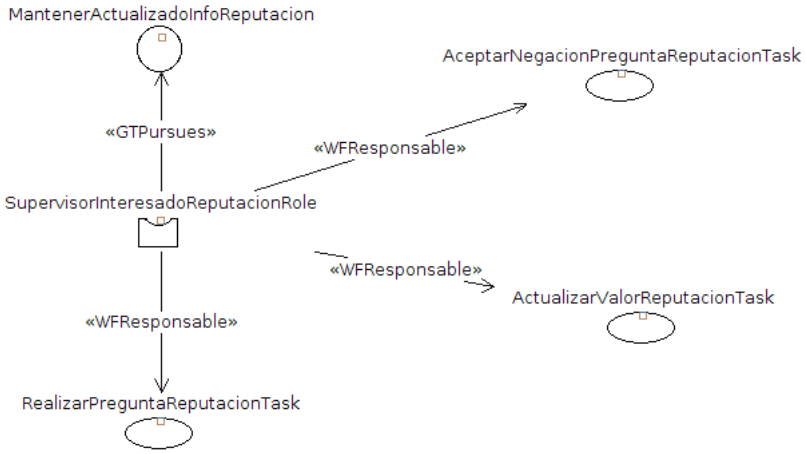


Figura 3.9: Modelo del Rol: Supervisor Interesado en Información de Reputación de un Agente

la información de reputación de testigos directos respecto a un agente colaborador determinado.

«RealizarPreguntaReputacionTask» (ver figura 3.10) es para la realización de la pregunta al resto de supervisores proveedores de información de reputación. Esta tarea se activa al recibir un hecho del tipo «ReputacionAgenteNecesaria». Tenga en cuenta que este hecho se genera cuando se recibe una propuesta de un agente (ver figura 3.4).

«ActualizarValorReputacionTask» (ver figura 3.11) es para actualizar la información de reputación de una agente específico cuando llegan respuestas de los demás supervisores ante la pregunta anterior.

Y finalmente «AceptarNegacionPreguntaReputacionTask» (ver figura 3.12) es para tratar con las respuestas negativas de los supervisores que desconocen al agente sobre el cual se preguntó.

3.3.4. El Rol: Supervisor Proveedor de Información de Reputación de Agente

El rol «SupervisorProveedorInfoReputacionRole» (ver figura figura 3.13) es la parte que responde ante las preguntas de los demás supervisores sobre la reputación de un agente colaborador.

Dicho rol consta únicamente de una capacidad, la tarea «ProcesarConsultaReputacionTask» (ver figura 3.14). Esta tarea se encarga de procesar la pregunta sobre la reputación de un agente específico, y elaborar la respuesta.

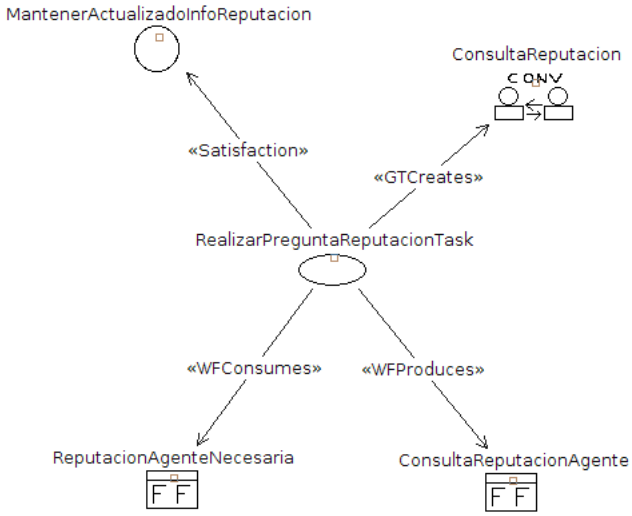


Figura 3.10: Modelo de la Tarea: Realizar Pregunta sobre la Reputación de un Agente

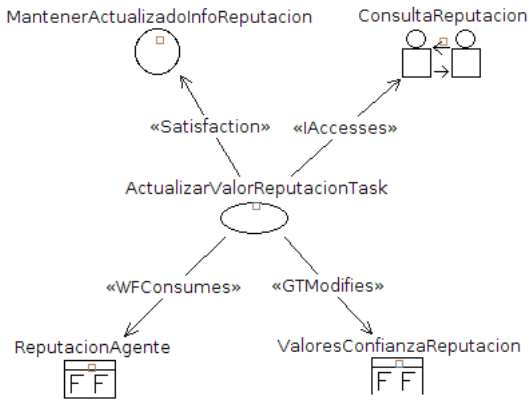


Figura 3.11: Modelo de la Tarea: Actualizar el Valor de Reputación de un Agente

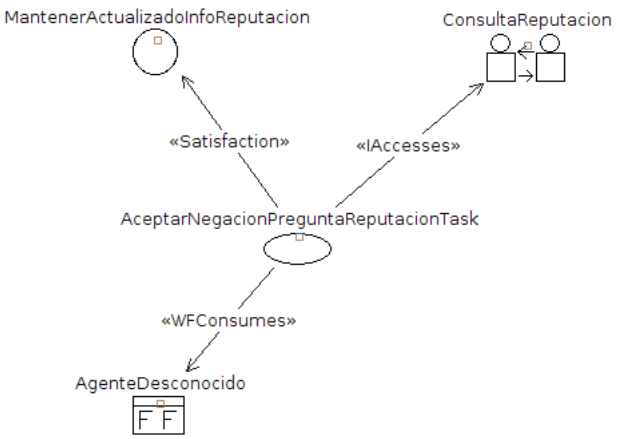


Figura 3.12: Modelo de la Tarea: Aceptar Negación de la Pregunta sobre la Reputación de un Agente

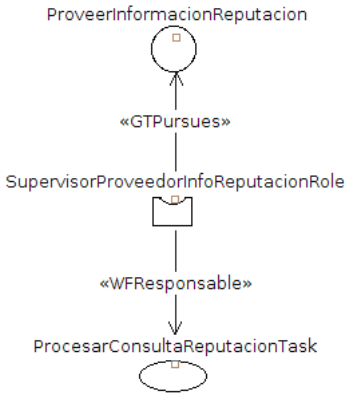


Figura 3.13: Modelo del Rol: Supervisor Proveedor de Información de Reputación de un Agente

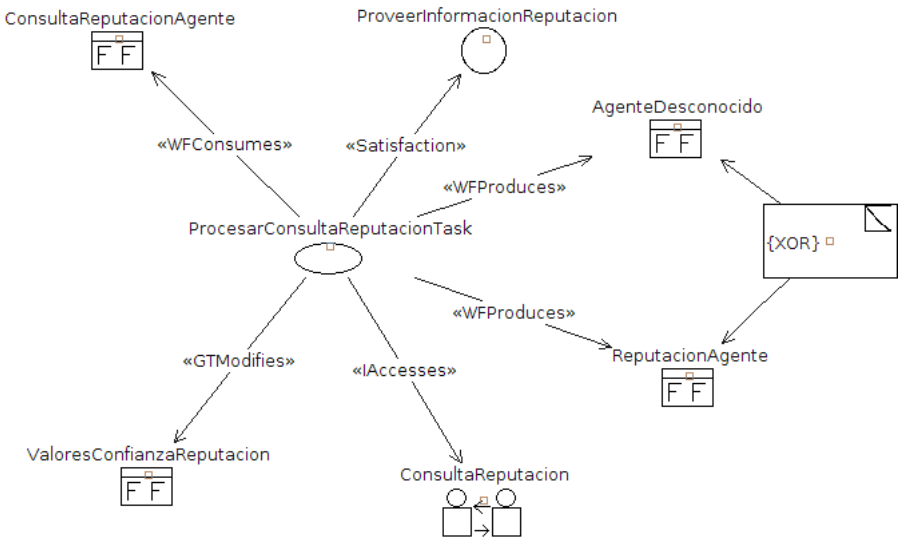


Figura 3.14: Modelo de Tarea: Procesar Consulta de la Reputación de un Agente

3.3.5. El Rol: Colaborador

El rol «ColaboradorRole»(ver figura 3.15) proporciona la capacidad de sugerir fuentes al sistema.

Este rol tiene en total tres tareas: «GenerarPropuestaTask», «ProcesarRespuestaPropuestaAceptadaTask» y «ProcesarRespuestaPropuestaRechazadaTask».

La tarea «GenerarPropuestaTask»(ver figura 3.16) se activa cada vez que aparece un hecho del tipo «NuevaPropuestaPorEnviar». Esta tarea prepara una propuesta de fuente para ser enviada a algún supervisor. Para ello crea una conversación del tipo «RealizacionPropuesta».

Finalmente, según el hecho que aparece en la respuesta de la conversación se activa la tarea «ProcesarRespuestaPropuestaAceptadaTask»(ver figura 3.17) o la tarea «ProcesarRespuestaPropuestaRechazadaTask» (ver figura 3.18), con el fin de tratar adecuadamente la respuesta recibida.

3.3.6. Los Roles: Colaborador Humano y Colaborador Artificial

Los roles «ColaboradorHumanoRole» y «ColaboradorArtificialRole» forman parte de una clasificación específica para el prototipo desarrollado en el ámbito de este trabajo. En otros dominios puede haber distintos tipos de Colaboradores Humanos y distintos tipos de colaboradores Artificiales con capacidades distintas o especializadas; o incluso otra forma de clasificación por capacidades extras aparte de la de interactuar con Supervisores.

El Rol «ColaboradorHumanoRole» extiende al «ColaboradorRole» ya que también tiene las capacidades de generar propuestas y de interactuar con los supervisores pero añade una capacidad más, ésta es la de interactuar con el usuario para validar la información introducida antes de ser tratada como propuesta.

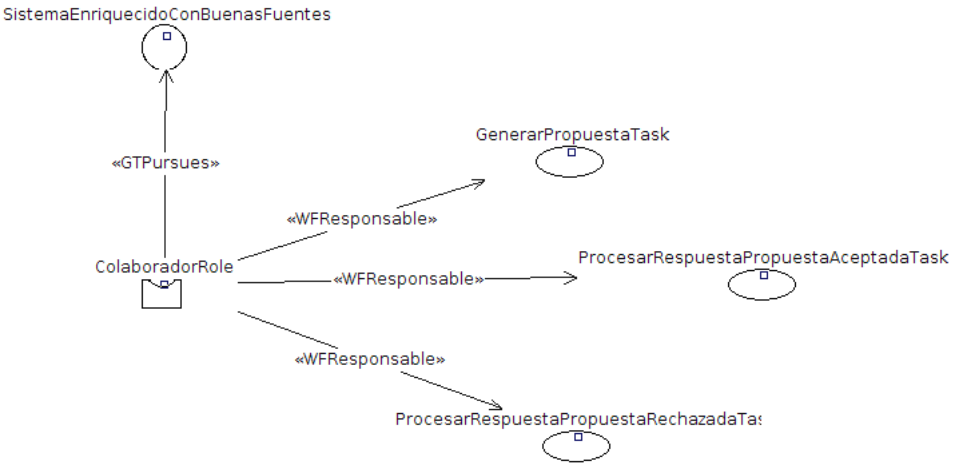


Figura 3.15: Modelo del Rol: Colaborador

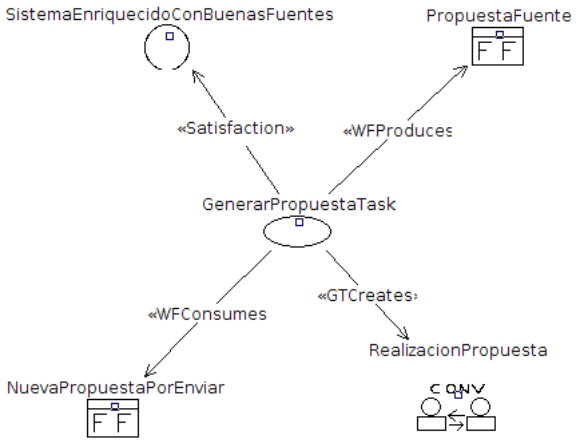


Figura 3.16: Modelo de la Tarea: Generar Propuesta

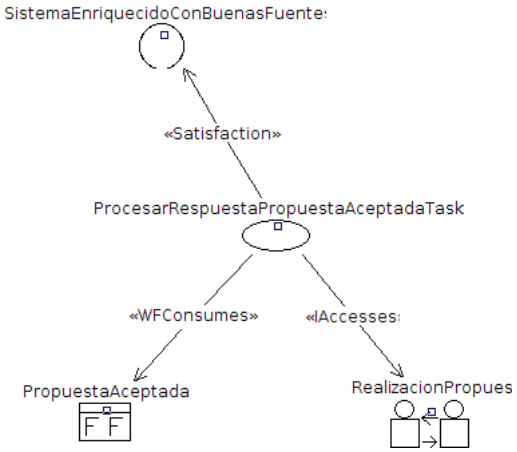


Figura 3.17: Modelo de la Tarea: Procesar Respuesta Propuesta Aceptada

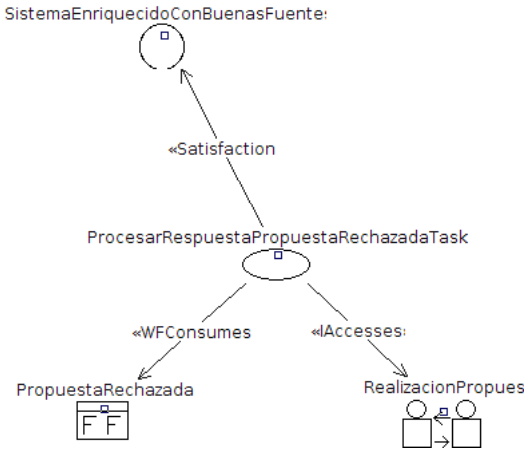


Figura 3.18: Modelo de la Tarea: Procesar Respuesta Propuesta Rechazada

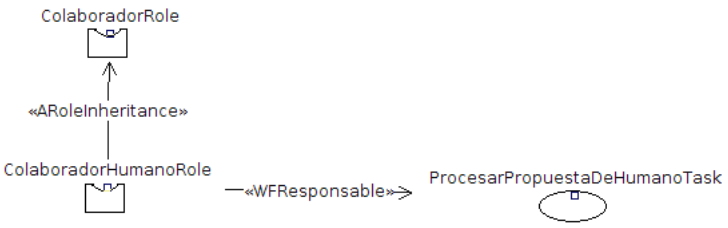


Figura 3.19: Modelo del Rol: Colaborador Humano

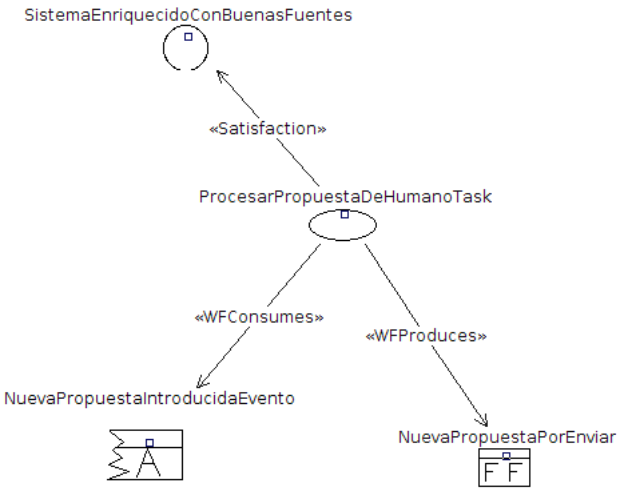


Figura 3.20: Modelo de Tarea: Procesar Propuesta de Humano

En la figura 3.19 se describe este rol y en la figura 3.20 se describe la tarea «ProcesarPropuestaDeHumanoTask» que corresponde con la capacidad descrita.

El Rol «ColaboradorArtificialRole» extiende también al «ColaboradorRole» ya que tiene las capacidades de generar propuestas y de interactuar con los supervisores pero añade la capacidad de buscar de manera autónoma nuevas fuentes de información para proponer.

En la figura 3.21 se describe el modelo del rol y en la figura 3.22 se describe el modelo de la tarea «BuscarFuenteTask».

Para la realización del prototipo, se han desarrollado dos agentes que juegan estos roles. Uno de ellos es el «AsistenteInvestigador» y el otro es el «ColaboradorAutonomo»(ver figura 3.23).

En la figura se describe el modelo de la tarea «InicializarVisualizacionTask» del agente «AsistenteInvestigador».

3.3.7. El Resto de Roles y Agentes

Este modelo preliminar es incompleto. Para darle una consistencia mínima, que además permita hacer un prototipo de implementación, se han desarrollado

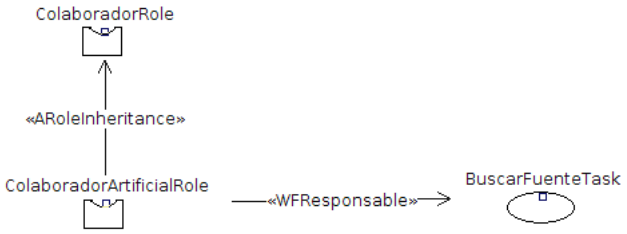


Figura 3.21: Modelo del Rol: Colaborador Artificial

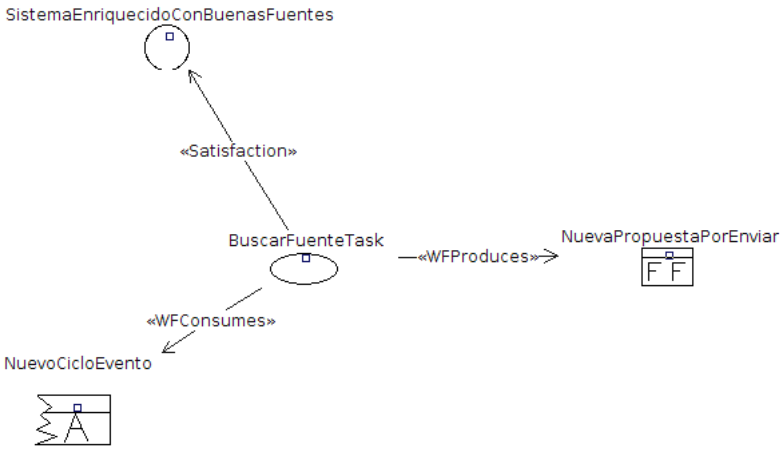


Figura 3.22: Modelo de la Tarea: Buscar Fuente

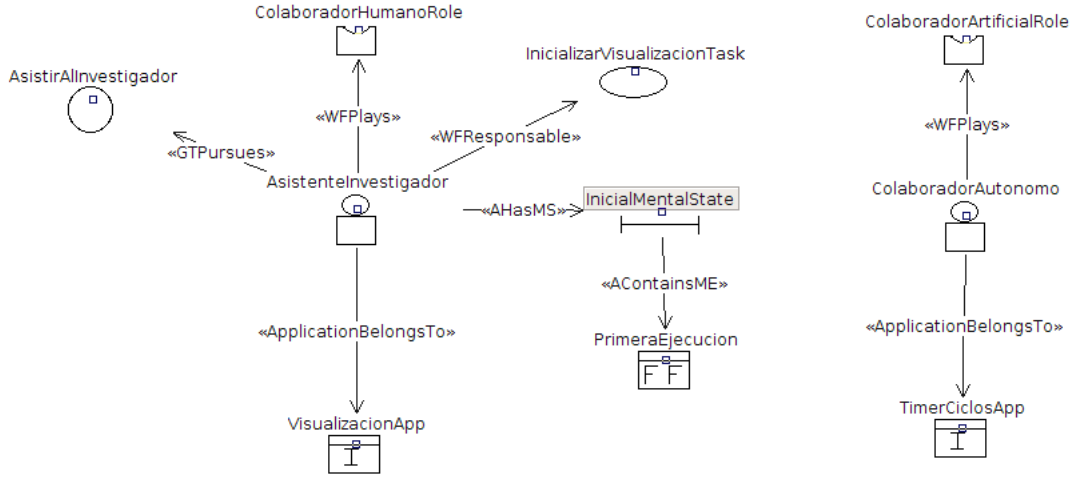


Figura 3.23: Modelo de Agentes: Asistente del Investigador y Colaborador Autónomo

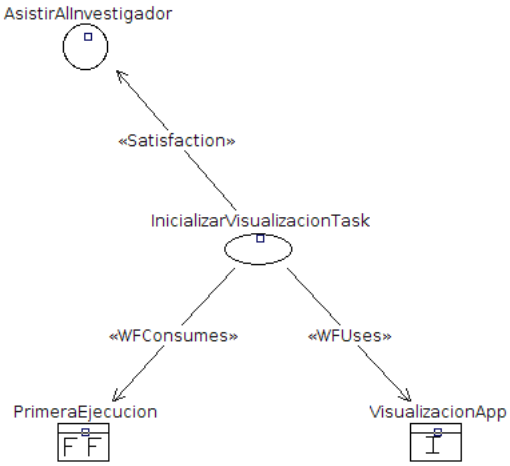


Figura 3.24: Modelo de la Tarea: Inicializar Visualización

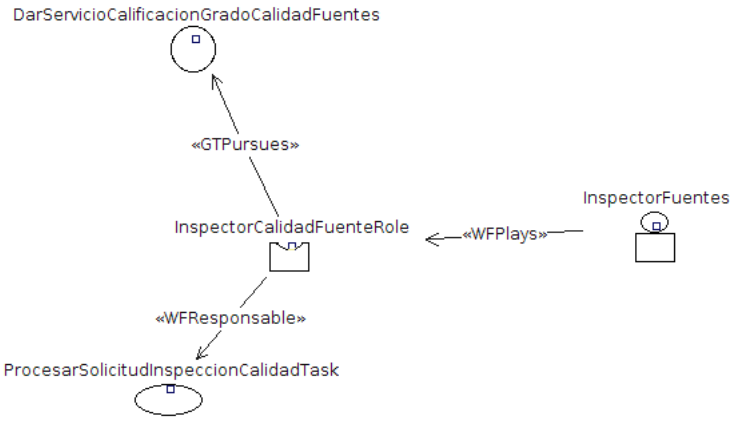


Figura 3.25: Modelo del Agente: Inspector de Fuentes

algunos agentes que simulan comportamiento y respuestas coherentes.

Dichos agentes son «InspectorFuentes», «GestorFuentes» y «InspectorAlfaFuentes».

En las figuras 3.25 y 3.26 se describen los modelos que conciernen al «InspectorFuentes». Este agente juega el rol «InspectorCalidadFuenteRole» y este a su vez solo contiene la tarea «ProcesarSolicitudInspeccionCalidadTask» que consume el hecho «InspeccionarCalidadFuente» que indica que se ha solicitado una inspección y produce el hecho «GradoCalidadFuente» que contiene el grado de calidad ya calculado. Este hecho es luego enviado de respuesta en la interacción de solicitud de inspección de calidad (ver sección 3.4).

En las figuras 3.27 y 3.28 se describen los modelos que conciernen al «GestorFuentes».

El agente «GestorFuentes» juega el rol «GestorFuentesRole». Este rol contiene solo una tarea llama «ProcesarPeticionIntroducirFuenteTask» la cual tiene como fin

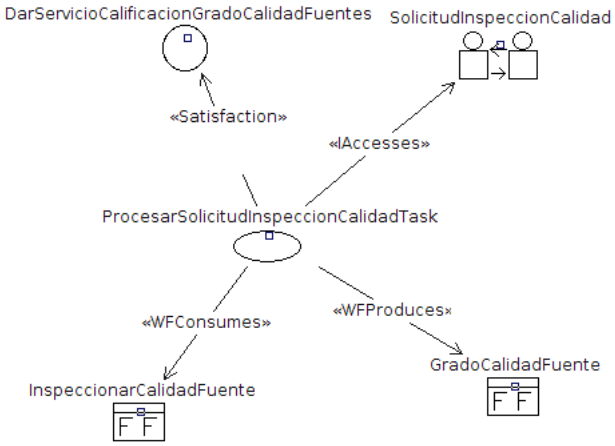


Figura 3.26: Modelo de la Tarea: Procesar la Solicitud de Inspección de Calidad

introducir las fuentes en el sistema para ser vigiladas.

En las figuras 3.29 y 3.30 se describen los modelos que conciernen al «InspectorAlfaFuentes».

Este agente juega el rol «InspectorAlfaCalidadFuenteRole» y este contiene la tarea «ProcesarSolicitudInspeccionAlfaCalidadTask» que consume el hecho «InspeccionarCalidadFuenteCuarentena» y produce el hecho «GradoCalidadFuenteCuarentena» que contiene el grado de calidad calculado. Este hecho es luego enviado de respuesta en la interacción de solicitud de inspección alfa de calidad (ver sección 3.4).

3.4. Modelos de Interacciones

A continuación se describen los modelos de las interacciones más relevantes.

3.4.1. La Propuesta de Fuentes

En las figuras 3.31, 3.32 y 3.33 se describe el modelo de interacción para la realización de propuestas por parte de colaboradores.

Como describen las figuras, la interacción consta de dos roles, el «ColaboradorRole» y el «SupervisorRole». Siendo el «ColaboradorRole» el agente que colabora proponiendo la fuente y siendo «SupervisorRole» el agente que decide si aceptar la propuesta o no.

La interacción está basada en el protocolo «Propose» del estándar FIPA [11], donde el acto del habla `propose` se utiliza para comunicar la propuesta y los `acept-proposal` y `reject-proposal` para comunicar la decisión de aceptación o rechazo de la propuesta.

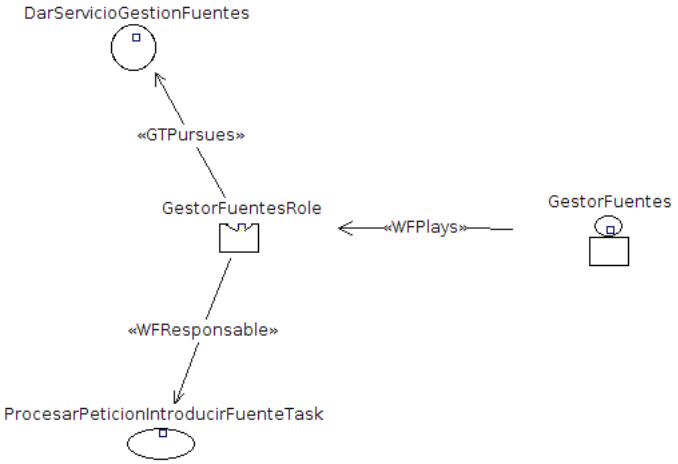


Figura 3.27: Modelo del Agente: Gestor de Fuentes

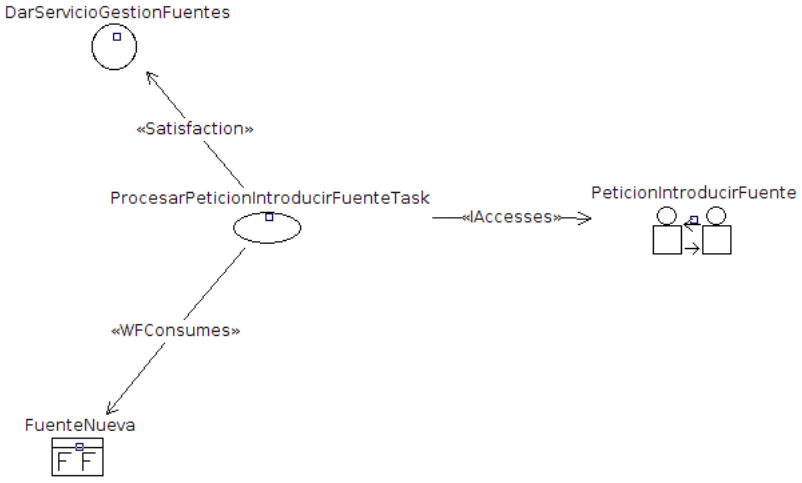


Figura 3.28: Modelo de la Tarea: Procesar Petición de Introducir una Fuente

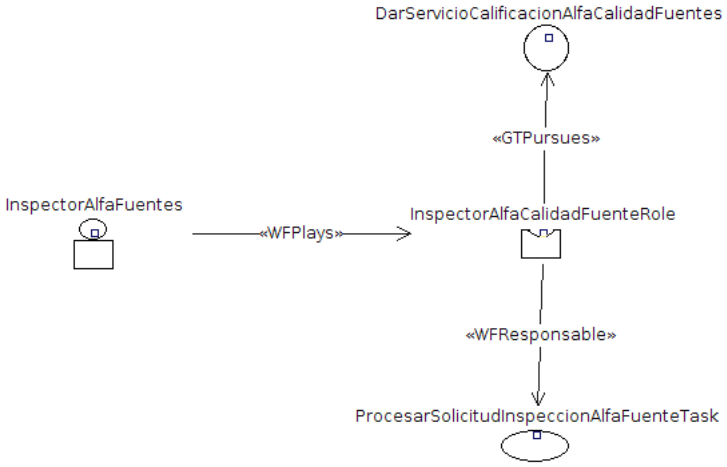


Figura 3.29: Modelo del Agente: Inspector Alfa de Fuentes

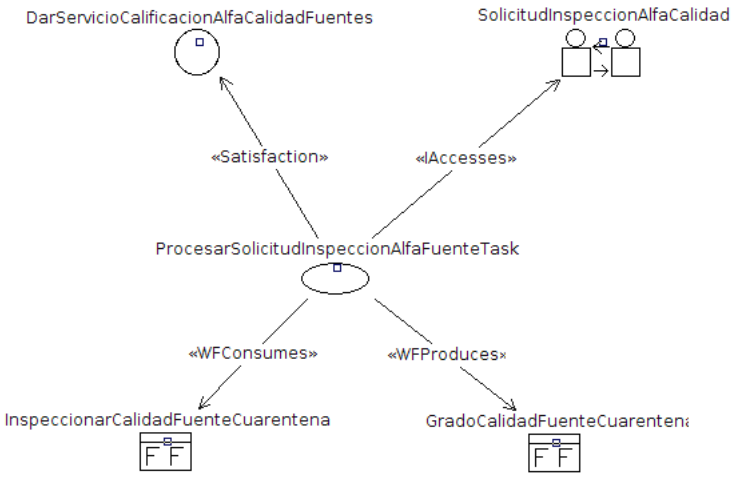


Figura 3.30: Modelo de la Tarea: Procesar Solicitud de Inspección Alfa de Calidad

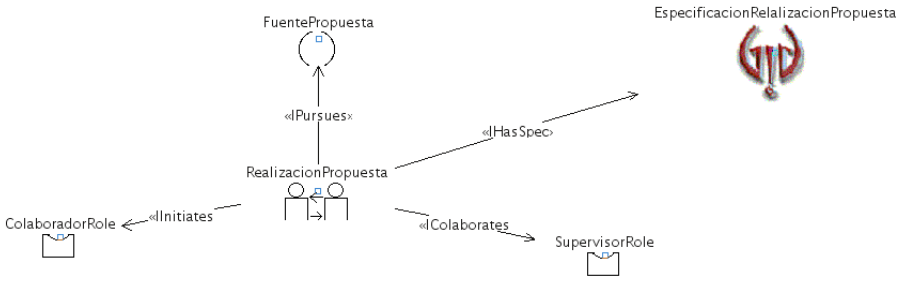


Figura 3.31: Modelo de Interacción para Propuesta de Fuente (1)

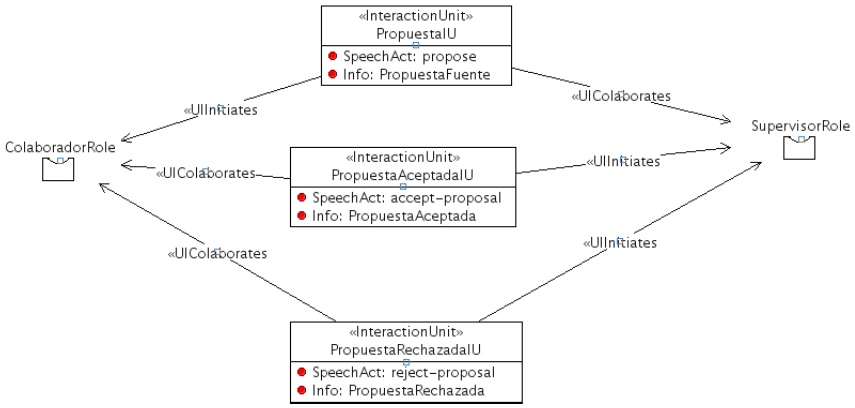


Figura 3.32: Modelo de Interacción para Propuesta de Fuente (2)

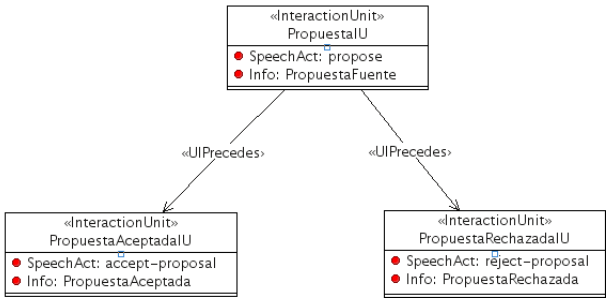


Figura 3.33: Modelo de Interacción para Propuesta de Fuente (3)

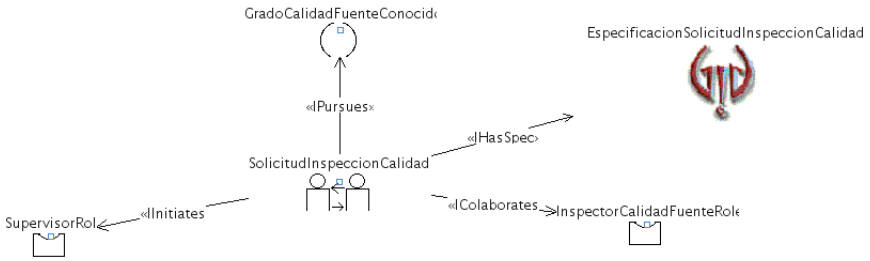


Figura 3.34: Modelo de Interacción para la Solicitud de Inspección de Calidad de una Fuente (1)

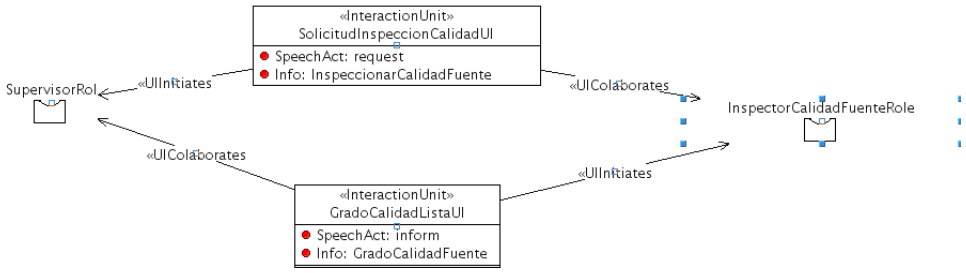


Figura 3.35: Modelo de Interacción para la Solicitud de Inspección de Calidad de una Fuente (2)

3.4.2. La Solicitud de Inspección de Calidad

Las figuras 3.34, 3.35 y 3.36 describen en tres partes el modelo de interacción de solicitud de inspección de calidad.

El protocolo de la interacción está basado en el estándar FIPA «Request», donde el acto del habla `request` comunica la solicitud de ejecución de la inspección de calidad y el `inform` comunica el resultado de la operación.

En este modelo de interacción participan dos roles, «SupervisorRole» y el «InspectorCalidadFuenteRole». El primero de ellos es el agente cliente del servicio que da el segundo.

3.4.3. La Petición de Introducir Fuente

En las figuras 3.37, 3.38 y 3.39 se describe el modelo de interacción para introducir fuentes en el sistema para ser vigiladas.

El protocolo de la interacción está basado en el estándar FIPA «Request», donde el acto del habla `request` comunica la petición de introducir la fuente en el sistema y el `inform` comunica el resultado de la operación.

En este modelo de interacción participan dos roles, «SupervisorRole» y el «GestorFuenteRole». El primero de ellos es el agente cliente del servicio que da el segundo.

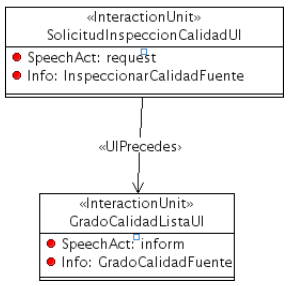


Figura 3.36: Modelo de Interacción para la Solicitud de Inspección de Calidad de una Fuente (3)

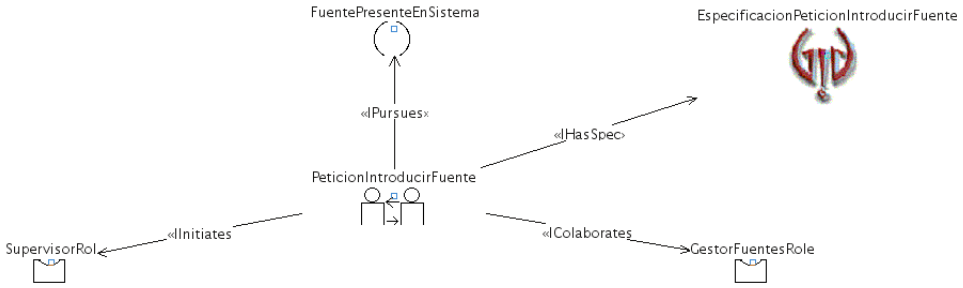


Figura 3.37: Modelo de Interacción para la Petición de Introducir una Fuente en el Sistema (1)

El resultado final de esta interacción es que la fuente dada por el agente «SupervisorRole» está en el sistema lista para ser vigilada.

3.4.4. El Intercambio de Información de la Reputación de un Agente

Las figuras 3.40, 3.41 y 3.42 describen en tres partes el modelo de interacción para el Intercambio de Información de la Reputación de un Agente.

Este modelo está basado en la especificación del protocolo «Query» del estándar FIPA. Donde el acto del habla `query-ref` comunica la pregunta sobre la reputación que un agente determinado. El acto del habla `refuse` comunica al que consulta que no se conoce tal agente y el acto del habla `inform` comunica la reputación que el agente tiene.

En esta interacción participan dos roles, «SupervisorInteresadoReputacionRole» y «SupervisorProveedorInfoReputacionRole». El primero de ellos es el que pregunta al segundo sobre la reputación de un agente determinado.

3.5. Modelo de Control del Filtrado

La lógica para seleccionar los filtros a aplicar a una propuesta está basada en un sistema de confianza y reputación sobre los colaboradores. Específicamente para

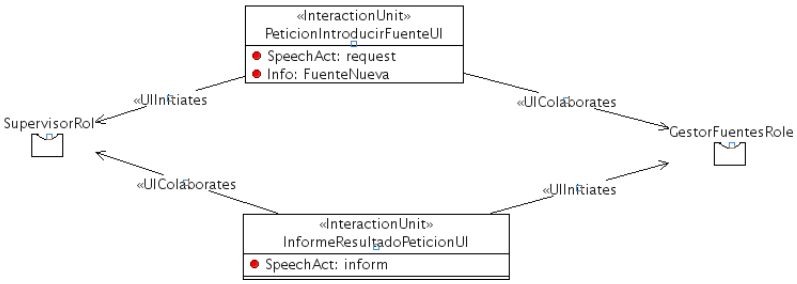


Figura 3.38: Modelo de Interacción para la Petición de Introducir una Fuente en el Sistema (2)

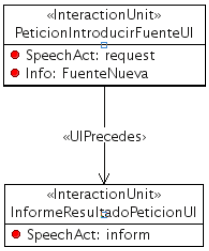


Figura 3.39: Modelo de Interacción para la Petición de Introducir una Fuente en el Sistema (3)

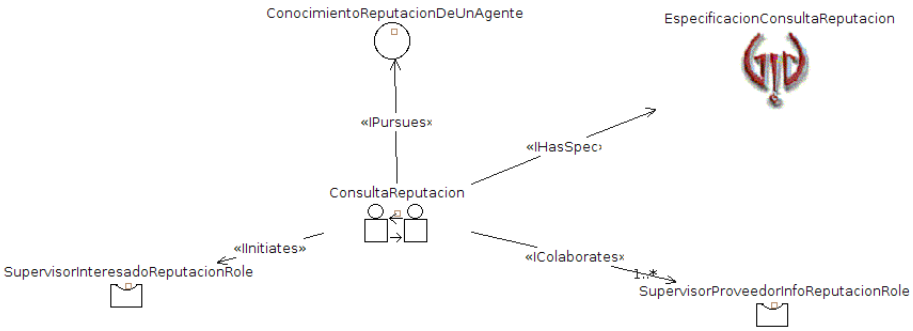


Figura 3.40: Modelo de Interacción para el Intercambio de Información de la Reputación de un Agente (1)

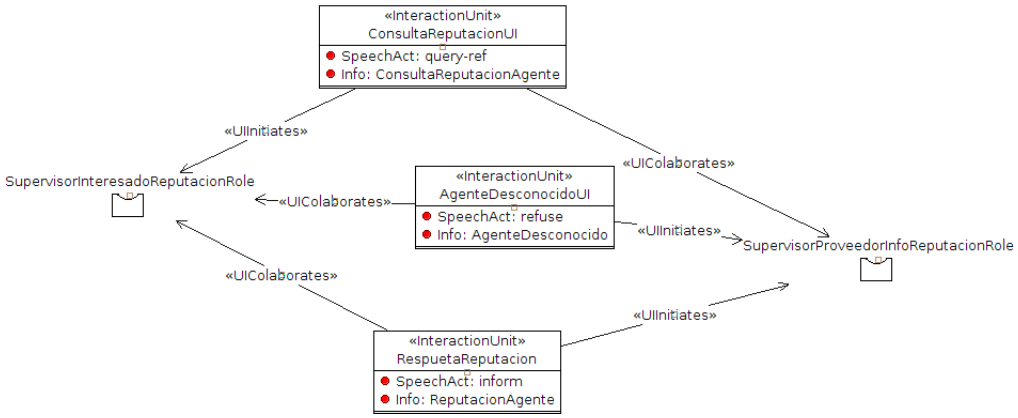


Figura 3.41: Modelo de Interacción para el Intercambio de Información de la Reputación de un Agente (2)

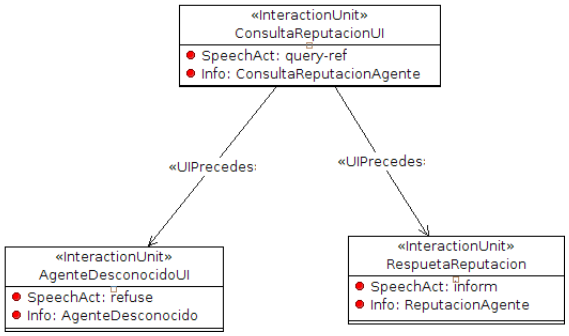


Figura 3.42: Modelo de Interacción para el Intercambio de Información de la Reputación de un Agente (3)

Grado de Confianza	Interpretación
$Trust_{a\to b}(\varphi) < 0$	El colaborador b suele proponer fuentes de baja calidad en cuanto al criterio φ
$Trust_{a\to b}(\varphi) \simeq 0$	El colaborador b suele proponer fuentes de calidad en cuanto al criterio φ
$Trust_{a\to b}(\varphi) > 0$	El colaborador b suele proponer fuentes de alta calidad en cuanto al criterio φ

Cuadro 3.1: Interpretación de los Grados de Confianza de un agente supervisor a sobre un agente colaborador b

este modelo preliminar se ha optado por implementar el sistema REGRET [28] con algunas simplificaciones. Esta elección se debe a que REGRET es suficientemente completo para el modelo preliminar que se ha propuesto. Quizás en trabajos futuros esta elección es sustituida por otra que incorpore nuevas características necesarias.

En este caso concreto los términos del contrato son los criterios indicadores de la calidad de una fuente, estos son: *Object-criteria*, *Process-criteria* y *Subject-criteria*. Para el cálculo de cada uno de ellos se realiza una media con pesos de cada uno de los valores de sus componentes. Para simplificar el cálculo, los agentes encargados de dar una valoración de la calidad darán valores en el rango $[-1, 1]$ en cada uno de los componentes de los indicadores, siendo el 1 «muy bueno/muy alto» y el -1 «muy malo/muy bajo». Para este modelo preliminar estos pesos serán iguales para cada componentes de los indicadores.

Inicialmente se establecen unos valores mínimos esperados para cada término del contrato (en el sistema REGRET se habla de contratos entre agentes con términos fijados al principio, con sus respectivos valores mínimos exigidos). Estos valores mínimos determinan el comportamiento esperado de cada colaborador, es decir, se espera que los colaboradores propongan fuentes con valores de calidad iguales o superiores a los mínimos en cada uno de los tres términos.

Se han realizado dos simplificaciones en el uso de REGRET. Estas son:

- Se le ha dado una credibilidad de 1 a todos los supervisores.
- La única reputación que se tendrá en cuenta es la reputación de testigos directos (*Witness Trust*)

El grado de confianza de la experiencia directa (*Direct Trust*) se calcula a partir de los valores de los indicadores de calidad de las fuentes propuestas en el pasado. Finalmente, la confianza final se calcula a partir del grado de confianza de la experiencia directa y de la reputación que tiene el colaborador en el resto de supervisores.

La interpretación que se le da a los grados de confianza es la mostrada en el cuadro 3.1.

El agente supervisor actuará de la siguiente manera a la hora de realizar el control y decidir si pasa la propuesta a ser procesada o no.

$$Pasa = \bigwedge_{\varphi \in \{\varphi_o, \varphi_p, \varphi_s\}} CtrlFiltro(\varphi, f)$$

$$CtrlFiltro(\varphi, f) = \begin{cases} True & EvalTrust(\varphi) \\ Filtrado(\varphi, f) & c.c. \end{cases}$$

$$EvalTrust(\varphi) = (Trust_{a \to b}(\varphi) \geq 0 \wedge TrustRL_{a \to b}(\varphi) \geq 0{,}5) \vee TrustRL_{a \to b}(\varphi) < 0{,}5$$

$$Filtrado(\varphi, f) = \begin{cases} True & Min(\varphi) \leq GradoCalidad(\varphi, f) \\ False & c.c. \end{cases}$$

Donde:

- $Pasa \in \{True, False\}$. Indica si una fuente pasa o no pasa a se vigilada por el sistema.
- f. La fuente a filtrar.
- $TrustRL_{a \to b}(\varphi)$. Fiabilidad del valor del grado de confianza que tiene el agente a en el agente b.
- $\varphi_o, \varphi_p, \varphi_s$. Términos del contrato *Object-criteria*, *Process-criteria* y *Subject-criteria* respectivamente.
- $GradoCalidad(\varphi, f)$. Calcula el grado de calidad de la fuente f respecto al término del contrato φ.
- $Min(\varphi)$. Valor mínimo exigido para el término del contrato φ.

La evaluación de la expresión primera se realiza de manera «perezosa».

En este modelo de control, la parte más costosa generalmente es la función *GradoCalidad*. Esta función se ejecutará únicamente cuando el valor del grado de confianza respecto a un término del contrato indica que se han introducido fuentes con grados de calidad por debajo de los mínimos en el pasado (o cuando no se tiene información suficiente para «prejuzgar» el comportamiento del agente colaborador) y es necesario medir la calidad de la fuente en este aspecto antes de introducirse finalmente en el sistema..

Si el grado de calidad calculado supera los mínimos entonces sí se introduce en el sistema.

En este trabajo se ha optado por tener el umbral de fiabilidad aceptable para tomar decisiones en el 0,5. Esto es porque la probabilidad de equivocarse ya comienza a ser menor para valores iguales o superiores. Para dominios específicos puede ser más adecuado tener valores mayores.

Este modelo de control es implementado por los agentes supervisores. El cálculo del *GradoCalidad* se delega a un agente especializado perteneciente al Equipo de Pruebas.

Capítulo 4

Conclusiones

En este trabajo se ha abordado la temática de los Sistemas de Vigilancia Tecnológica y los Agentes Inteligentes.

La Vigilancia Tecnológica, enmarcada en el concepto de Inteligencia Competitiva, contiene un conjunto de procesos que en la literatura y en el estándar UNE 166006:2006 EX se tratan de definir. En este trabajo se ha desarrollado una definición orientada a la automatización informática del Sistema de Vigilancia Tecnológica.

A partir de dicha definición se ha realizado una exploración para estudiar la utilidad de los modelos de confianza para evaluar la calidad de las fuentes de información gestionadas en Sistemas de Vigilancia Tecnológica y la aplicabilidad del enfoque de agentes para el desarrollo de estos sistemas.

Los Sistemas de Vigilancia Tecnológica se nutren de fuentes de información sobre los cuales realizan la vigilancia. Dichas fuentes de información pueden llegar a partir de los mismos investigadores, ya que estos suelen tener bien localizadas buenas fuentes de información. En esta línea se han estudiado técnicas de confianza y reputación en sistemas multiagentes para la selección del conjunto mínimo de filtros necesarios para las propuestas de fuentes de información.

Se ha desarrollado un modelo preliminar multiagente que implementa la aplicación selectiva de filtros sobre propuestas de fuentes utilizando técnicas de confianza y reputación. Para ello se ha utilizado la Metodología y las Herramientas de INGENIAS.

De esta forma, se ha podido evaluar a la vez la facilidad de uso del concepto de agente para diseñar estos sistemas al mismo tiempo que se estudia la forma de integrar los modelos de confianza. Aunque no se han podido recoger una medida exhaustiva del uso de estos modelos, sí que se ha podido constatar que en los escenarios considerados, el sistema se comporta como se espera intuitivamente y como marca el modelo de confianza. Sin embargo, sería conveniente una experimentación más precisa y a más largo plazo para determinar si operarios humanos aprecian cambios positivos en la información suministrada con y sin modelos de confianza.

El diseño orientado a agentes que se hizo usando la Metodología INGENIAS permitió crear un sistema con entidades software autónomas y cooperativas gracias al manejo de conceptos como Objetivos, Tareas e Interacciones. La autonomía y la cooperación se ve, por ejemplo, en los agentes Supervisores. Estos agentes tiene

el objetivo de mantener el sistema con fuentes de calidad, y para ello deciden que operaciones hacer en cada propuestas sin intervención del usuario. Estas decisiones están sujetas al aprendizaje (por la experiencia directa) y a la cooperación en grupo (por la reputación). El análisis orientado a agentes también permitió crear un sistema que computan de manera distribuida y se coordinan de manera asíncrona. Y finalmente, permitió crear un sistema flexible al cambio gracias al concepto de Rol y a la comunicación por mensajes.

El uso de la Metodología y las Herramientas de INGENIAS para modelar el sistema multiagente que implementa el filtrado ha sido satisfactorio. Las notaciones específicas del dominio de agentes inteligentes facilitaron y agilizaron el proceso de análisis y diseño del modelo. El desarrollo en código Java del prototipo ejecutable fue rápido gracias a las herramientas de generación de código ejecutable de INGENIAS y a su Framework IAF[1]. El código ejecutable generado, así como el Framework IAF dan implementado todo el control interno del agente, la correlación de mensajes en las conversaciones, la gestión de entidades mentales, la verificación de las precondiciones de ejecución de tareas, entre otras.

Sin embargo, no hay notaciones específicas para la confianza y la reputación en INGENIAS. Esto se ha suplido especificando explícitamente las interacciones y las entidades necesarias para la gestión de la confianza y la reputación. Con notaciones específicas se pudiera modelar de manera sencilla los escenarios de intercambio de información de los distintos tipos de reputación, sin tener que hacer todo el modelado de las interacciones y de la gestión de la información de reputación, de manera explícita. Por ejemplo, una asociación del tipo «Trusting» que relaciona dos roles. Esto indicaría que el agente del rol origen calculará confianzas a partir de experiencias directas con el agente del rol destino, y que los agentes del rol origen compartirán información de reputación sobre los agentes del rol destino de la asociación. Esta asociación tendría que tener algún «feature» que indicase la interacción sobre la que se obtiene la experiencia directa. Evidentemente faltan más cosas por detallar sobre este tema para hacer una propuesta completa, pero no es el objetivo final de este trabajo.

El Framework IAF puede además ser extendido para darle soporte a la confianza y la reputación entre agentes. Esta extensión sería la gestión semi-automática de la confianza y la reputación. Una notación específica en el modelo podría indicar al Framework que se ha de activar este aspecto en el sistema multiagente generado. Esta notación específica puede ser la misma que se ha propuesto en el párrafo anterior.

4.1. Trabajos futuros

A modo de síntesis, a continuación se describen los posibles trabajos futuros derivados de este trabajo de investigación.

- Completar el modelo de filtrado de propuestas. En concreto, cómo los agentes inspectores de calidad obtienen la información necesaria para calcular el valor

[1] Framework para agentes y sistemas multiagentes incluido en las Herramientas de INGENIAS

de los distintos parámetros de calidad. Falta la interacción con los usuarios y con los expertos.

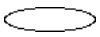
- Desarrollar modelos para la arquitectura software global del Sistema de Vigilancia Tecnológica. Estos modelos deben tener en cuenta las distintas características necesarias del sistema como la pro-actividad, la autogestión, la autonomía, entre otras.
- Proponer notaciones en INGENIAS para la confianza y reputación en sistemas multiagentes.
- Desarrollar extensiones del Framework IAF para la gestión semi-automática de la confianza y la reputación.

Apéndice A

Introducción a la Metodología INGENIAS

INGENIAS[22] es una Metodología acompañada de herramientas software para el desarrollo de Sistemas Multiagentes.

En el cuadro A.1 se describen algunas de las notaciones utilizadas en este proyecto.

Notación	Descripción
	Representa una organización de agentes
	Representa un grupo de agentes
	Representa un rol que puede ser jugado por agentes
	Representa una interacción entre agentes
	Representa un agente
	Representa una tarea
	Representa un objetivo
	Representa un hecho
	Representa un evento
	Representa una aplicación interna al sistema multiagente

Cuadro A.1: Algunas Notaciones de INGENIAS utilizadas en éste trabajo

Bibliografía

[1] Grupo CDE - Inteligencia Competitiva. URL: http://www.cde.es [20 abril 2009].

[2] Madri+d - Vigilancia Tecnológica. URL: http://www.madrimasd.org/vigTecnologica/ [21 abril 2009].

[3] Miguel A. Valero, José A. Sánchez, and Ana Belén Bermejo. Informe de Vigilancia Tecnológica madri+d "Servicios y tecnologías de teleasistencia: tendencias y retos en el hogar digital". Technical report, Fundación madri+d para el Conocimiento, Madrid, 2007.

[4] AENOR. UNE 166006:2006 EX: Gestión de la I+D+i: Sistema de Vigilancia Tecnológica. Final, UNE, 2006.

[5] Yue-Shan Chang, Yu-Cheng Luo, and Pei-Chun Shih. AIR: Agent and Ontology-Based Information Retrieval Architecture for Mobile Grid. In *APSCC '08: Proceedings of the 2008 IEEE Asia-Pacific Services Computing Conference*, pages 650–655, Washington, DC, USA, 2008. IEEE Computer Society.

[6] Ken Conttrill. Turnin Competitive Intelligence into Business Knowledge. *Journal of Business Strategy*, 19, Julio/Agosto 1998.

[7] Paul Degoul. Introducción práctica a la problemática de la vigilancia tecnológica en las PYMES. In *Conferencia en LEIA*, Parque Tecnológico de Miñano, Victoria, 2000. Centro de Desarrollo Tecnológico.

[8] Pere Escorsa and Ramon Maspons. *De la vigilancia tencológica a la inteligencia competitiva*. Prentice Educación, S.A., Madrid, 2001.

[9] Barbara Ettorre. Managing Competitive Intelligence. In *Management Review*, volume 84. 1995.

[10] Ronen Feldman and Ido Dagan. Knowledge Discovery in Textual Database (KDT). In *KDD-95*. AAAI, 1995.

[11] Foundation for Intelligent Physical Agent. FIPA Specifications. Final, IEEE Computer Society, 2002.

[12] Juan Garbajosa Sopeña and Francisco Javier Soriano Camino. Informe de Vigilancia Tecnológica madri+d "Tecnologías software orientadas a servicios". Technical report, Fundación madri+d para el Conocimiento, Madrid, 2008.

[13] Trung Dong Huynh, Nicholas R. Jennings, and Nigel R. Shadbolt. An integrated trust and reputation model for open multi-agent systems . In Springer Netherlands, editor, *Autonomous Agents and Multi-Agent Systems*, volume 13, pages 119–154. September 2006.

[14] François Jakobiak and Henri Dou. *La veille technologique*, chapter De l'information documentaire à la vielle technologique pour l'entreprise: enjeux, aspects généraux et définitions. Dunod, Paris, 1992.

[15] Vicente Julián, Adriana Giret, and Vicente J. Botti. *Agentes Software y Sistemas Multiagentes. Conceptos, Arquitecturas y Aplicaciones*, chapter 6.4. Aplicaciones en recuperación de información, pages 221–231. Pearson Education, S.A., 2005.

[16] Matthias Klusch. Information agent technology for the Internet: A survey. *Data and Knowledge Engineering*, 36(3):337–372, March 2001.

[17] L. Mui, M. Mohtashemi, and A. Halberstadt. A computational model of trust and reputation. *System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on*, pages 2431–2439, Jan. 2002.

[18] Felix Naumann and Claudia Rolker. Assessment Methods for Information Quality Criteria. In *Proceedings of the International Conference on Information Quality*, pages 148–162, 2000.

[19] Fernando Palop and José Miguel Vicente. *Vigilancia tecnológica e Inteligencia competitiva. Su potencial para la empresa española*. COTEC, Madrid, 1999.

[20] Ron Papka, James Allan, and Victor Lavrenko. UMASS Approaches to Detection and Tracking at TDT2. In *DARPA Broadcast News Transcription and Understanding Workshop*, pages 111–116, Herndon, Virginia, 1999. DARPA.

[21] Juan Pavón, Francisco Garijo, and Jorge Gómez-Sanz. Complex Systems and Agent-Oriented Software Engineering. In Springer Berlin Heidelberg, editor, *Engineering Environment-Mediated Multi-Agent Systems*, volume 5049/2008 of *Lecture Notes in Computer Science*, pages 3 – 16. SpringerLink, Julio 2008.

[22] Juan Pavón, Jorge J. Gómez-Sanz, and Rubén Fuentes-Fernández. *The INGENIAS Methodology and Tools*, article IX, pages 236–276. Idea Group Publishing, 2005.

[23] Kanagasabi Rajaraman and Ah-Hwee Tan. Topic Detection, Tracking, and Trend Analysis Using Self-Organizing Neural Networks. In *PAKDD 2001*, pages 102–107. Springer-Verlag Berlin Heidelberg, 2001.

[24] Sarvapali Dyanand Ramchurn. *Multi-Agent Negotation using Trust and Persuasion*. Phd thesis, School of Electronics and Computer Science, University of Southampton, December 2004.

[25] J. M. Reagle Jr. *Trust in a cryptographic economy and digital security deposits: Protocols and policies*. Master of science thesis, Departament of Technology and Policy, MIT, 1996.

[26] María Jesús Rivas Martínez. Informe de Vigilancia Tecnológica madri+d "Gestión térmica de sistemas espaciales". Technical report, Fundación madri+d para el Conocimiento, Madrid, 2009.

[27] Daniel Rouach. La Veille Technologique et l'Intelligence Ëconomique. In *Que sais-je?*, volume 3086. Presses Universitaires e France, Paris, 1996.

[28] J. Sabater. *Trust and Reputation for agent societies*. Phd thesis, Universitat Autónoma de Barcelona, 2003.

[29] Jordi Sabater-Mir, Mario Paolucci, and Rosaria Conte. Repage: REPutation and ImAGE Among Limited Autonomous Partners. *Journal of Artificial Societies and Social Simulation*, 9, 2006.